MITRE

SWIM Core Architecture Evolution Concepts

Version 1.0

Ezra Jalleta

Bindu Kaul

Duncan Thomson

July 2009

CAASD

MITRE

SWIM Core Architecture Evolution Concepts

Version 1.0

Ezra Jalleta
Bindu Kaul
Duncan Thomson

July 2009

Approved By:

MITRE Department Approval:

———————————————————————

Lisandro del Cid
Program Manager

MITRE Project Approval:

———————————————————————

Frank W. Buck
Outcome Leader

Abstract

This document provides strawman System Wide Information Management (SWIM) Core Architecture Evolution Concepts with primary focus on Segment 2. Functional architecture is discussed which is based on the National Airspace System (NAS) Enterprise Services functional hierarchy created as part of the NAS Enterprise Architecture Framework development effort. There is brief mention of the technical architecture, which is intended to be filled-in later as the technical standards to be used in Segment 2 become better understood. The document contains an analysis of options for components that may be deployed and interconnected by the SWIM program in Segment 2 in order to realize the functional architecture. The intent is to identify these components and discuss their advantages and disadvantages so that subsequent requirements analysis and cost estimation can be performed. Options in different areas are combined into two overall SWIM Segment 2 architecture options with the federated approach for Segment 1 given as a third option. Pros and cons of the options are presented, and a preliminary recommendation is made.

Keywords: SWIM Segment 2 Architecture, NGIP, NextGen, SWIM Evolution, SWIM, Enterprise Architecture, NAS Information Systems Security, SWIM Core

Table of Contents

List of Figures

List of Tables

1 Introduction

The Federal Aviation Administration (FAA) System Wide Information Management (SWIM) Program concept is to provide an open and flexible information management architecture that facilitates sharing of operational data among National Airspace System (NAS) entities in a secure and manageable fashion (SWIM Final Program Requirements - Segment 1 May 2007). The information shared includes flight, traffic flow management (TFM), aeronautical information, and weather data. To achieve this, NAS applications will have to migrate toward a loosely coupled net-centric computing environment in order to realize cost and risk reduction in the development of services and add life and value to NAS applications through reuse.

Design and development efforts for the first step to implement this concept are now underway in SWIM Segment 1. At the same time the next step, SWIM Segment 2, is being conceived and planned.

As has been discussed in detail in various SWIM documents including the SWIM Segment 1 Technical Overview document (FAA, System Wide Information Management (SWIM) Technical Overview, Version 1.1 March 2008), a federated approach was taken for the implementation of SWIM Segment 1. This means SWIM Implementing Programs (SIPs) implement and operate SWIM Core Capabilities, mission services (e.g., flight and weather), and data services. To facilitate interoperability and seamless interface among SIP SWIM systems, the SWIM Program provided a common suite of software that offers a common set of core capabilities such as messaging and a central service registry capability.

The SWIM Segment 2 vision discussed in Section 2 of this document considers the possibility of deploying hardware and software that would support a "SWIM Core" infrastructure in order to move closer to a NAS net-centric infrastructure. This NAS net-centric infrastructure would include:

- Service Oriented Architecture (SOA) infrastructure layer
- Basic information technology (IT) infrastructure
- Information system security (ISS) infrastructure

In line with this vision, the architecture presented in subsequent sections captures SWIM Core Architecture concepts and identifies infrastructure improvements and evolution path alternatives. The architecture contained herein is focused primarily on SWIM Segment 2, although with the intent of providing a solid foundation for future segments leading to the complete net-centric NAS envisioned in the Next Generation Air Transportation System (NextGen) Concept of Operations (Joint Planning and Development Office-FAA June 2007).

Various inputs were used for the analysis including Operational Concepts for SWIM in the Mid-term (Boan and others September 2008) and NAS Security Architecture (Signore and others 2009) concepts.

1.1 Purpose and Scope

The purpose of this document is to develop SWIM Core architecture evolution concepts which will primarily form the basis for the development of SWIM Segment 2 core architecture. The architectural options contained in this document are intended be used to support the SWIM Segment 2 planning process including the SWIM Segment 2 Joint Resources Council (JRC) decision in mid 2010. The main focus of the document is an analysis of options for components that may be deployed and interconnected by the SWIM program in Segment 2 in order to realize the functional architecture. These components may include hardware and software subsystems. The intent is to identify subsystems so that further requirements analysis and cost estimation can be performed and a final set of SWIM Segment 2 requirements can be identified.

The architecture contained in this document is a strawman. After a period of reviews and feedback it will be updated to reflect inputs from stakeholders and eventually become the SWIM Segment 2 Technical Overview document.

1.2 Approach

Various inputs formed the basis for the development of SWIM Segment 2 architectural alternatives, including:

- Concept of Use for SWIM in the Mid-Term (Prabhu and Thomson March 2009)

- Analysis of Next Generation Implementation Plan (NGIP) Solution Sets for SWIM

- NAS Enterprise Architecture Service Description Framework

- SWIM Segment 2 Operation Services and Environment Definition (OSED) (SWIM Segment 2 Operation Services and Environment Definition, Version 1.0 March 2009)

- SWIM Segment 1 Architecture

- NAS Security Architecture

- Ongoing SIP work

- Industry Consortium Report (GEIA) input for SWIM Segment 1 to Segment 2 transition (FAA SWIM Program - Segment 1 to Segment 2 Transition - Industry Input December 2008)

- Joint Planning and Development Office (JPDO) Net-Centric Working Group

Our analysis began with adopting a functional architecture based on the NAS Enterprise Architecture enterprise services functional decomposition. Architectural components available to provide these functions were identified based on available and emerging technology and the components currently being designed in SWIM Segment 1. One or more options were identified for each core service. Grouping together meaningful combinations of options from the different areas led to the development of two overall options along with a third option which entailed the federated architecture from Segment 1. The pros and cons of these options were analyzed and summarized. Finally, we formed a preliminary recommendation based on these pros and cons.

1.3 Document Organization

Section 2 sets the context for the rest of the document. It covers SWIM vision and mission need, the rationale for NAS net-centric infrastructure, industry recommendations, and acquisition and operations concepts for SWIM Segment 2.

Section 3 details the functional architecture envisioned for SWIM Segment 2 which is based on SWIM functions derived from the NAS Enterprise Services Architecture Framework.

Section 4 is a place-holder for the SWIM Technical Architecture which will be more completely defined prior to Segment 2 design efforts.

Section 5 is the main body of the document. A set of capabilities that, together, provide the functions included in the functional architecture are analyzed. For each of these capabilities, we analyze the factors that will drive the architectural decisions, then present a set of options for components (notional hardware and software subsystems) to realize these capabilities.

Section 6 provides a summary of overall architectural alternatives along with the pros and cons of each and a preliminary recommendation.

Discussion of NAS Information System Security Architecture is included in the Appendix B.

2 Background

2.1 SWIM Vision and Mission Need

The SWIM mission need is captured in (FAA, Exhibit 300: Attachment 3, Implementation Strategy and Planning, System Wide Information Management (SWIM) Program, Initial Submission June 2007) . Some key statements from that document are:

> "The purpose of SWIM is to facilitate net-centric NAS operational improvements, as proposed by the JPDO's Next Generation Air Transportation System, with far less expense and complexity than required by current methods."

> "Today's hard-wired infrastructure and systems cannot readily support the addition of new data, systems, data users, and/or decision makers as NextGen requires."

> "The SWIM Program is an integral part of the NAS Enterprise Architecture roadmap and will [promote] a secure NAS-wide information web to connect FAA systems. Furthermore, it will enable interaction with other members of the decision-making community including other agencies, air navigation service providers, and airspace users."

From the same document the Program Strategy in Segment 1 and beyond is summarized as:

> "In Segment 1, the strategy is to have the implementing programs use existing NAS platforms to the maximum extent feasible for hosting SWIM software."

> "In later SWIM Segments, it may be necessary to deploy separate hardware and/or software in order to support the SWIM infrastructure."

Based on these statements of mission need and program strategy, and reinforced by several studies referenced here, we are led to a vision for the evolution of SWIM depicted in Figure 2-1. In Segment 1, the SWIM program facilitated a move towards standards-based information exchanges among NAS systems, with new interfaces implemented within these systems by the SIPs. In Segment 2, to continue the evolution towards meeting the stated mission need, and in accordance with the stated program strategy, we believe the next step is to begin to implement a NAS net-centric infrastructure. This NAS net-centric infrastructure should include a SOA infrastructure layer, referred to in this document as the "SWIM Core". Deployment and operation of the SWIM Core would be the primary responsibility of the SWIM program. Net-centric infrastructure also includes basic IT infrastructure (e.g., LAN and WAN network infrastructure) and ISS infrastructure (e.g., identity and key management). SWIM may have a role in these latter infrastructure layers, working together with other programs such as the FAA Telecommunications Infrastructure (FTI) program and, possibly, the Logical Access and Authorization Control Service (LAACS) program. Subsequent segments of SWIM are expected to continue to add capabilities to the NAS net-centric infrastructure and possibly expand its scope to include, for example, air/ground information exchanges.
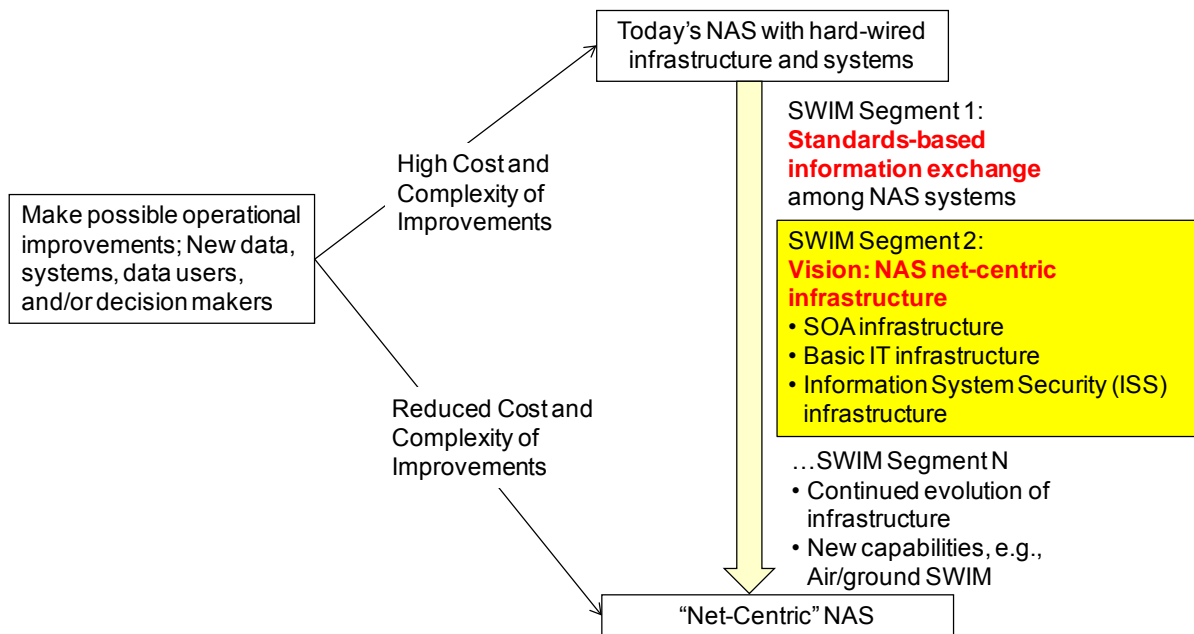
Figure 2-1. Vision for SWIM Evolution

2.2 Rationale for NAS Net-Centric Infrastructure

As discussed above, this document is based on a vision in which SWIM, in Segment 2, begins to implement a NAS net-centric infrastructure. In this section we provide additional rationale for this vision.

The following factors point to the value of evolving from the purely federated architecture used in SWIM Segment 1 toward a consolidated or hybrid architecture that includes a centrally provided and operated SWIM Core:

1. The existence of a SWIM Core facilitates "Loose Coupling".

Without a SWIM Core, NAS end systems interface directly with other NAS end systems. Adoption of SWIM standards simplifies the definition and development of these interfaces, but SIPs must still work pairwise with other SIPs to create interface agreements and define points of presence for accessing SIP services. The existence of the SWIM Core makes available a different paradigm, in which SIPs and the SWIM program work out agreements for information to be "on-ramped"[1] from SIP-developed end systems to the SWIM Core. Once the information is available within the SWIM Core, it is available to be accessed by other users and systems that are connected to the SWIM Core, without the producer and consumer having to develop and agree upon a new interface between their respective end systems. Data owners retain control of who is allowed to access their information through centrally managed policy-based access

---

[1]   The term "on-ramp" has been used in the FTI program prototyping activities to refer to the concept of transferring information from NAS end systems to a central facility, from which it can be further disseminated as needed.

control mechanisms supported by the SWIM core, rather than pairwise control over which NAS end system is allowed to access which other NAS end system.

Note that at this point we are not advocating that *all* information must pass through the SWIM Core – SIPs can still directly access other SIPs' services when and if there is a good reason to do so.

2. **Reduced time to deploy new information management capabilities into the NAS.**

Once created, the SWIM Core provides a standards-based environment that can be used to rapidly deploy new services. There are many different ways in which such a capability might be used, but we envision two primary use cases. First, the SWIM Core may be used to rapidly create new capabilities for disseminating information products to consumers in new and useful forms. As we will see in Section 5, there is considerable technology that could be made available in the SWIM Core that allows information to be transformed, aggregated, filtered, routed, published/subscribed, and so on. These technologies allow extremely rapid development of new information dissemination capabilities. A second use case for the SWIM Core is to support new information processing applications that don't already have - and don't have a need for - a dedicated computing environment. By hosting these applications in the SWIM Core, a SIP can focus its domain expertise on defining the application-layer information processing functions, while allocating to the SWIM core issues such as computing hardware, operating system, security mechanisms, SOA software stack, and so on.

3. **Simplified system management and security**

System management and information system security functions are complex and difficult to implement, and may require 24x7 staffing by skilled system administrators. By offloading functionality to the SWIM Core, some SIPs may be able to reduce staffing costs for these functions. Furthermore, operators of the SWIM Core will have a more global view of operations across the entire NAS, and therefore better able to put together and end-to-end view of service performance and security.

4. **Total Cost of Ownership**

By centralizing and standardizing information management, the SWIM Core has the potential to reduce costs in some areas, such as:

- Lower license costs
- Efficient resource utilization through pooling
- Reduced redundancy of procurement effort
- Reduced redundancy of engineering effort
- Reduced redundancy of operations planning and development effort
- Increased resource utilization for operations

- Increased resource utilization for hardware and software

- Increased efficiency with respect to test and interoperability

These factors and others have been examined and analyzed in previous work, and the results generally support the arguments for the value of beginning to implementing a net-centric infrastructure in Segment 2. Previous work in this area includes:

1. *Program strategy approved at JRC.* As discussed above, Segment 1 relies on SIPs to implement capabilities within existing platforms, but separate hardware and software was recognized as potentially needed for SWIM in later segments.

2. *SWIM Segment 1 architecture.* As documented in (FAA, System Wide Information Management (SWIM) Technical Overview, Version 1.1 March 2008) (FAA, System Wide Information Management (SWIM) Technical Overview, Version 1.1 March 2008) the system engineering team that created the Segment 1 architecture concluded that the desired end-state architecture for SWIM included consolidated infrastructure.

   "As the SWIM architecture continues to grow and mature, it is envisioned that consolidated components can be deployed as common, centralized infrastructure. This approach ensures standardization, better performance, lower total cost of ownership (TCO), and more consistent management of the SWIM infrastructure." (FAA, System Wide Information Management (SWIM) Technical Overview, Version 1.1 March 2008) (FAA, System Wide Information Management (SWIM) Technical Overview, Version 1.1 March 2008)

3. *Industry recommendation.* The (FAA SWIM Program - Segment 1 to Segment 2 Transition - Industry Input December 2008) recommends a "shared services infrastructure", which corresponds to what is referred to here as "net-centric infrastructure". (The GEIA industry recommendation is discussed further Section 2.3.)

4. *NAS Security Architecture.* The NAS Security Architecture, which is being developed at the time of this writing, calls for IT and ISS solutions to be architected as NAS-wide solutions, rather than as program-specific solutions, to reduce costs, decrease complexity, increase interoperability, and improve overall security. As will be seen in the discussion of ISS in Section 5.6, the creation of a NAS net-centric infrastructure facilitates the centralization of NAS ISS controls, consistent with the emerging NAS Security Architecture.

5. *Department of Defense (DoD) Experience.* DoD experience with established programs, such as Net-Centric Enterprise Services (NCES) and Global Combat Support System – Air Force (GCSS-AF) (Reed and McCaughin March 2009), as well as newer programs such as Consolidated Afloat Networks & Enterprise Services (CANES) (Department of the Navy August 2007), have shown that providing services in the form of consolidated infrastructure offers greater benefits than can be obtained from technical standards, technical guidance, standardized selection of Commercial off-the-Shelf (COTS) software, and governance and coordination activities, which was the approach taken in SWIM

Segment 1. In particular the GCSS-AF program has demonstrated how more significant benefits, especially from the perspective of an individual program, can be obtained if there exists an infrastructure to which program requirements can be allocated. In SWIM Segment 2 we seek to obtain greater benefits by making it possible for programs to offload requirements to the net-centric infrastructure, where they can be implemented and operated at a lower overall life-cycle cost.

2.3   Industry Recommendations for SWIM Segment 2

In the Information Technology Association of America (ITAA) recommended architecture, "Consolidated NAS mission services" are deployed onto a "Shared Services Infrastructure". This "Shared Services Infrastructure" relies on an underlying network infrastructure, as well as additional IT and ISS infrastructure (not shown) in order to perform its functions. Figure 2-2 shows how the "shared services infrastructure" concept from the ITAA (formerly GEIA) report equates to what we call the "NAS net-centric infrastructure".

Figure 2-2. NAS Net-Centric Infrastructure Relationship to GEIA Report

Using the scoring approach shown in Table 2-1, the GEIA report compares the Federated Core, Consolidated Core, and Shared Core Service models, and reaches the following conclusion:

"Shared Services architecture offers a reasonable number of advantages to the other, more extreme approaches, and thus should be chosen as the model for SWIM Segment 2." (FAA SWIM Program - Segment 1 to Segment 2 Transition - Industry Input December 2008)

2-5

Table 2-1. Industry Comparison of Service Models for Segment 2 and Beyond

	Federated Core Services	Consolidated Core Services	Shared Core Services
Flexible	3.6	2.9	4.7
Initial Cost	2.1	3.8	4.1
Management Cost	2.9	3.9	4.2
Service Portfolio Mgmt	2.7	3.8	4.1
Mgmt & Service desk	2.4	4.4	4.6
NAS Asset Utilization	2.8	2.8	4.8
Policy Mgmt	2.3	4.1	4.4
Scalability	3.3	3.3	4.9
Efficiency	2.9	3.9	4.6
Data Proliferation	2.7	3.9	4.6
Secure	3.3	3.8	4.4
Performance	3.4	2.9	4.6
Availability	2.8	3.7	4.3
Maintainability	2.2	3.4	4.0
Overall Grade	39.4	50.6	62.2

Grading

5 – Offers outstanding benefits
4 – Offers better-than-average benefits
3 – Offers average benefits
2 – Offers below-average benefits
1 – Fails to offer any net benefits

2.4   SWIM Segment 2 Development and Operations Concepts

The introduction of net-centric infrastructure implies a change in the way SWIM capabilities are developed and operated, as well as major implications for the SWIM Segment 2 architecture. This section touches briefly on the development and operations concepts, while architectural implications are the subject of the remainder of this document.

As background, Figure 2-3 provides an overview of the development and operations concepts for SWIM Segment 1. In SWIM Segment 1, requirements were generated based on a process that included input from SWIM communities of interest (COIs) working towards the NextGen vision for net-centric capabilities. This process resulted in JRC approval of funding to implement a set of requirements for SWIM Segment 1 capabilities. The SWIM program has selected a common suite of software (the SWIM "service container") that provides a set of core capabilities (e.g., messaging, security). The SIPs are responsible for developing mission services (e.g., flight services, weather services), which can be built using the core capabilities provided by the SWIM service container software to interface to data and processing resources within the NAS systems (e.g., ERAM, TFM). These mission services, made accessible over the FTI Internet Protocol (IP) network, will allow NAS systems to interoperate and share data. The SWIM core capabilities, mission logic, and data services, are implemented by SIPs, and operated and maintained by the same staff that operate and maintain the individual NAS systems.
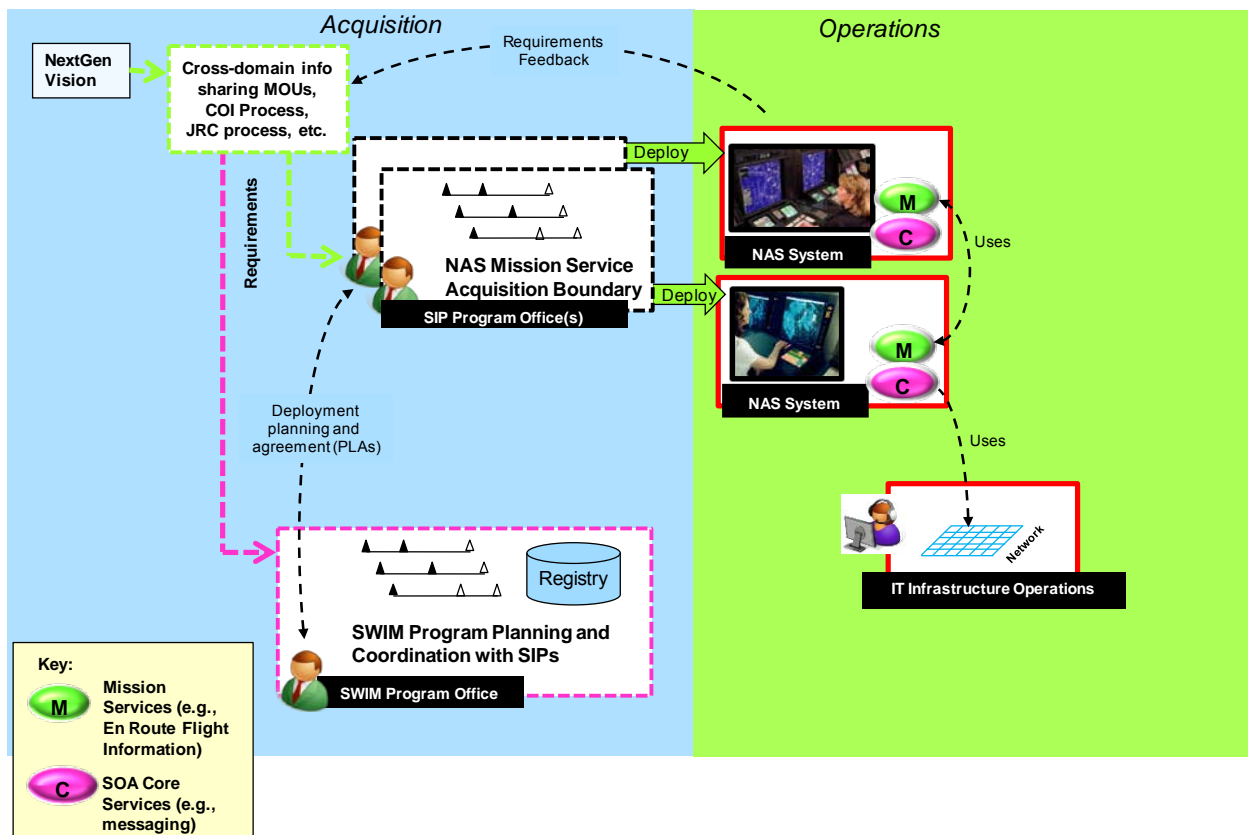
Figure 2-3. SWIM Segment 1 Development and Operations Overview

In contrast, a notional overview of the SWIM Segment 2 concept for development and operations is shown in Figure 2-4. The fundamental change in this concept is that the SWIM Program office now has responsibility to develop and deploy a "SWIM Core[2]" containing a set of consolidated core services. NAS mission services providing NAS data services may continue to be acquired, deployed, and operated within specific NAS systems, and these NAS systems continue to support SWIM SOA core services in a federated manner. However, in the hybrid model, some NAS mission services may be selected for deployment to the SWIM Core as the result of a NAS portfolio requirements allocation process. These are likely to be services that deal primarily with information dissemination and transformation, but may also include services that do not need to be hosted. In this case, these services, referred to as "Support Services," would still be developed by a NAS system program office with the necessary NAS mission subject matter expertise. However, rather than being hosted on hardware and software platforms within an existing NAS system boundary; these services would run on platforms provided by the SWIM Core.

The SWIM Core will utilize underlying network services, ISS resources, and computing resources (e.g., servers). These may be considered part of the SWIM Core, however for the

---

[2] Note that in the context of SOA prototyping activities conducted by FTI, the term "NAS Tier" has been used for what is referred to in this document as the "SWIM Core".

purposes of this architecture we consider these underlying resources to be provided as part of a separate "IT and ISS Core". The SWIM Core as well as the IT and ISS Core make up the NAS net-centric infrastructure.
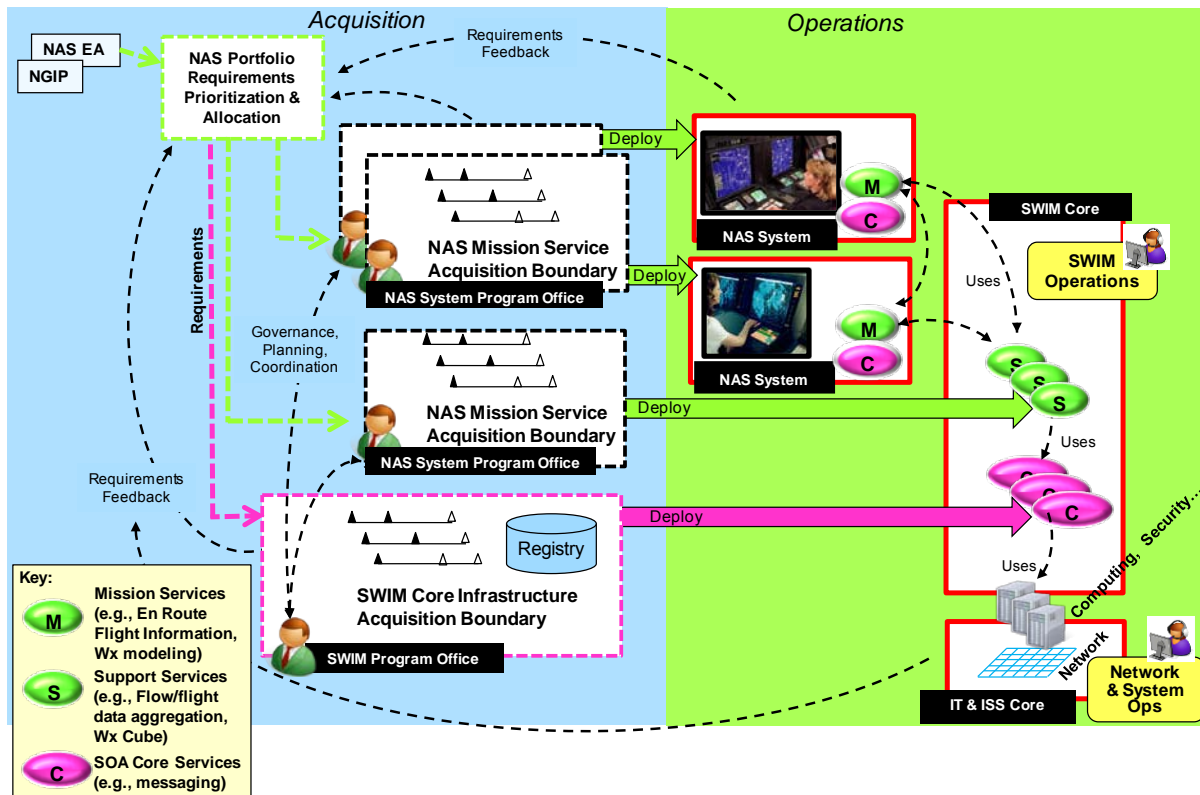
Figure 2-4. Notional SWIM Segment 2 Development and Operations Concept

The concepts shown in Figure 2-4 imply that some new roles and responsibilities and business models need to be worked out. The FAA must define the organizational entity or entities that are responsible for acquiring, deploying, administrating and operating the SWIM Core. This entity is referred to in this document as "SWIM Operations", and discussed in more detail in sections 3 and 5.

The responsibility for administrating and operating NAS IT and ISS infrastructure capabilities must also be clearly defined. Furthermore, a model of interaction between these entities and NAS end system operational support entities must be worked out. For example, in the acquisition domain, the SIPs and the SWIM program must agree on what Support Services are to be deployed to the SWIM Core, so that the appropriate core capabilities can be developed on a schedule that meshes with the SIP schedules. Integration testing facilities and processes must be created so that the correct operation of SIP-developed Support Services working in the SWIM Core environment can be assured before operational deployment. Once in operation, the operations support personnel in charge of specific Mission and Support Services must interact with those in charge of the SWIM Core and IT and ISS Core capabilities (SWIM Operations), so that problems can be quickly isolated and corrected.

3   SWIM Functional Architecture

In order to be consistent with other ongoing work, we have chosen to use a functional architecture that is based very closely on the NAS Enterprise Services functional hierarchy (SV-4) developed as part of the NAS Enterprise Architecture, and documented in the SWIM Core Services Enterprise Architecture Views Document, Draft Version 2.08, April 23, 2009 (SWIM Core Services Enterprise Architecture Views, Draft Version 2.08 April 2009). As we have developed our analysis, we have made some changes to the original SV-4, however we have tried to keep those changes to a minimum, and are feeding our changes back into the comment process in order to help the FAA converge on a common functional hierarchy.

The functional hierarchy is depicted in Figure 3-1. The horizontal layers in the figure represent operational functions that are carried out by entities within the NAS, and the vertical bars represent NAS wide processes and activities (including tools and capabilities) that are carried out (by people and organizations) to support the operational functions within the horizontal bars.
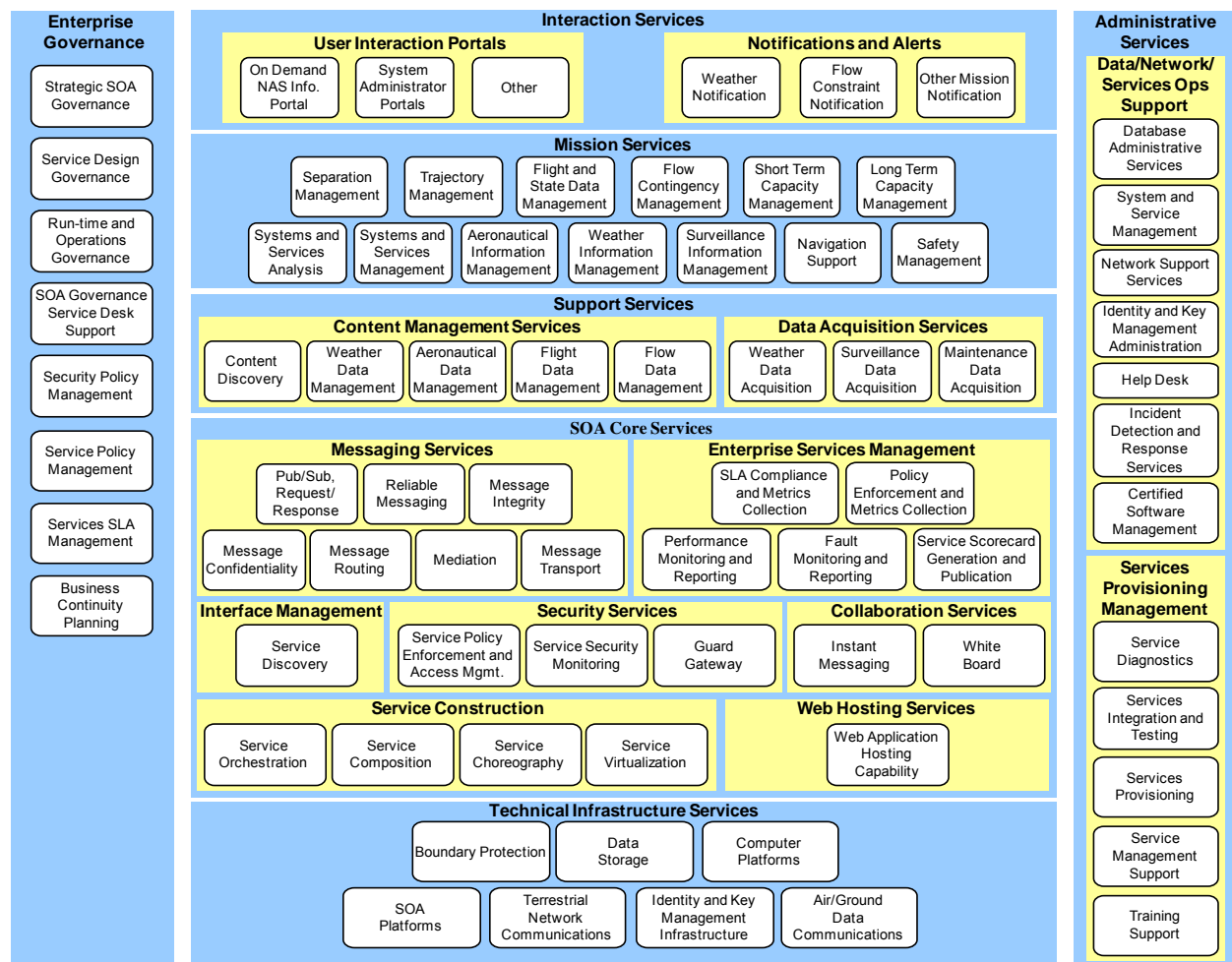
Figure 3-1. NAS Enterprise Services Functional Hierarchy (SV-4)

3-1

The following sections describe the functions from Figure 3-1 that are most pertinent to SWIM. While most of the functions that are discussed are categorized under SOA Core Services, other functions are also discussed, such as some that fall under Enterprise Governance.

3.1   Interaction Services

These are services that allow human users to interact with NAS information resources over a net-centric infrastructure. In the SWIM Segment 2 time frame these services are expected to be provided as web applications using web server technology, accessed by humans using a web browser. Note that the "Interaction Services" area includes the application level content and logic of these services; the underlying web hosting platforms are included in a lower layer. Interaction Services may be built using content provided by NAS Mission Services and Support Services, or may provide content to these services.

Interaction Services include User Interaction Portals, as well as Notifications and Alerts (e.g., Rich Site Summary (RSS) feeds).

3.2   NAS Mission Services

These are services that provide access to the information and resources essential to the operation of the NAS.

3.3   NAS Support Services

These are services that distribute information from NAS Mission Services. Support services may extract, aggregate, and transform information from Mission Services, as well as ensure that information is delivered to the right users, using lower level mechanisms such as publish/subscribe messaging, content based routing, and so on.

3.4   SOA Core Services

3.4.1   Messaging Services

SWIM Core Messaging is a common enabler for services, providing communication and messaging security. This enabler includes the sub-functions described in the following paragraphs.

3.4.1.1   Publish and Subscribe

Publish and subscribe messaging allows a publisher to send a single message to a messaging channel and have a copy of that message delivered to all the consumers who have subscribed to the message channel. The publisher sends a message to the messaging channel and does not wait for the reply from any of the subscribed consumers before proceeding.

3.4.1.2   Request and Response Messaging

Request and Response message allows a requester to send a request to a service provider and then to receive a response from the provider. In case of failure of request, either a failure response is sent by the service provider or the provider does not reply, in which case the request times out.

3.4.1.3   Reliable Messaging

Failures and errors can interrupt messaging between applications. Messages can be lost, duplicated or reordered. Service providers and service consumers can experience system failures and lose volatile state. Reliable messaging functionality in applications allows a reliable messaging source to accurately determine the disposition of each message it transmits to a destination and to resolve any in-doubt status regarding receipt of the message that was transmitted.

3.4.1.4   Message Routing

A message routing function sends messages to different destinations based on a set of conditions that are applied to a message after being consumed from a message channel. The most common type of message routing is *Content-Based* Routing, where the message destination depends on the contents of the message itself. Another type is *Context-based* message routing, where message destination is based on environment conditions. Context-based routers are used in load-balancing, parallel processing, and failover functionality. Another type is *Itinerary-based message routing*, which is based on metadata that is carried with a message (e.g., a list of forwarding addresses or rules that are evaluated at each endpoint processing the message).

3.4.1.5   Message Mediation

Messaging within an enterprise and with external partners results in interactions of different data models, formats, and transports between the sender and the receiver. A common message data format and transport used in all messaging interactions may not be practically feasible. The message mediation functions allow messages to be transformed to overcome this problem. At the application level, custom code can be written to transform the message structurally. Data types (e.g., numeric to string, time-zones) and formats (e.g., eXtensible Markup Language (XML), comma separated values, name-value pairs) can be parsed and rendered in a different format. Decryption and Encryption are applied to message content where needed. Messages transmitted using different protocols (e.g., HTTP, JMS, TCP/IP) require transport mediation. Bridges and adaptors are usually used as mediators to provide the necessary message transformation.

3.4.1.6   Message Transport

Message transport is a mechanism by which messages are sent between applications. Some common examples of protocols used for message transport are:

- Simple Object Access Protocol (SOAP) over Hypertext and Transfer Protocol (HTTP)/HTTP over Secure Sockets Layer (SSL) (HTTPS): SOAP messages are carried over HTTP or HTTPS transport

- SOAP over Java Messaging Service (JMS) over HTTP/HTTPS: SOAP messages are carried over JMS. The JMS connection is tunneled through a firewall using HTTPS protocol. The secure protocol (HTTPS) also involves mutual authentication using digital certificates

- JMS over SSL: Tunneling of JMS connection through a firewall using SSL (secure socket layer) protocol which uses digital certificates for authentication

3.4.1.7 Messaging Security

This function includes Message Confidentiality and Message Integrity.

3.4.1.7.1 Message Confidentiality

Message confidentiality reduces the risk of someone other than the intended receiver understanding the message as it flows between applications. For confidentiality, the message is encrypted before it is sent and decrypted when it is received by the correct target.

3.4.1.7.2 Message Integrity

Message Integrity ensures that a sender's message data is not tampered with in transit to the receiver. To ensure that the un-modified message data is received by the intended receiver and not an imposter requires authentication between the sender and the receiver. Messages are encrypted to ensure message confidentiality and message integrity is achieved by sending a message digest with the encrypted message. Message digest is a fixed-length representation of a message, a fingerprint of the original message. The message fingerprint is verified on the receiver side, for message integrity. Whereas confidentiality refers to encryption, integrity refers to digital signing of messages. Digital signing delivers message integrity and by verification of the digital signature non-repudiation is also achieved.

3.4.2 Service Construction Capability

Building a robust NAS to support the NextGen vision will require connecting many information resources. To achieve flexibility and meet changing requirements, distributed resources need to be re-combined and services need to be re-assembled. A robust and secure messaging backbone supports the reformulation of services, by propagating the business events and workflows for broader access. New services can be consumed with minimal integration when enabled on the messaging infrastructure.

Service Construction is the additional capability used by applications on the messaging backbone of the *SWIM Core*. Existing services or applications are left in place and new services are built on the messaging backbone.

Service Orchestration is the modeling of a business process in which each step is specified as a technical process and the interaction between the different processes is also specified in a similar

fashion. Orchestration is the automation of the processes which invoke services in a particular order, following a defined set of rules to accomplish a higher business function.

Service Composition is the integration of services to a higher level composite service to be used in different functions and formats than the services that comprised it. There are *fine grained* services, which can be combined to form *coarse grained* service and further combined to form a *composite service*. A calculator example can clarify the definition of these terms. To support basic calculator functions, the operations (e.g., addition, subtraction, division, and multiplication of two numbers) would be the *fine grained* service. The *coarse grained service* of a calculator would include the mathematical operations and the service function to store the results. A calculator service in use, would invoke the *fine grained service* when adding, subtracting, etc. An accounting service would be a *composite service*, and includes a calculator service and other services used for its business functions.

3.4.3   Web Hosting Services

These services provide web application hosting functions. These functions provide a platform that can be used to deploy Interaction Services.

3.4.4   Collaboration Services

Collaboration services allow humans to work together on a shared task. Collaboration services may provide functions such as voice communications, instant messaging, white board with annotations, desktop or window sharing, and web conferencing.

3.4.5   Interface Management

The Interface Management core service functions include capabilities that enable service providers to publish information about services and service consumers to discover information about services. This information includes definition of the syntax and semantics of services and the data produced and consumed by services. Information about different versions of services and data schemas is also managed, as well as information about Service Level Agreements (SLAs). In addition to the basic publication and discovery functions, user registration and subscription for notification are also associated supporting functionalities.

3.4.5.1   Service Discovery/Registry

Service Discovery is a key element of Interface Management in SWIM SOA Core Services. It constitutes both Service Information Publication (Service Exposure) and the discovery of service information as enabled by a service registry. The basic design-time registry provides the capability for service consumers to easily find service endpoint information along with key attributes like service ownership and versions. Providers can also publish service information subject to Governance procedures.

3.4.6   Enterprise Governance

Several Enterprise Governance functions have been identified in Figure 3-1. Of those, only functions that have to do with managing policies and which are typically associated with service metadata repositories are discussed below. A service metadata repository is generally considered a governance tool because it has contract (or SLA) and policy management capabilities in addition to storing extended service artifacts. The registry and repository should generally be integrated and synchronized in handling information related to a given service. For the purposes of discussion in this document both are collectively referred to as the registry (in most discussions) and are managed by the same organization. Note that it is possible for different organizations to manage these elements while keeping them synchronized (e.g., group responsible for Governance and group responsible for design-time activity management or even operations).

3.4.6.1   Security Policy Management

Security Policy Management in the SOA context is a function that enables the storing, updating and distribution of service related security rules (e.g., allow or limit access to a service) established by a governance body. A governance body creates high level policies which are documented in a human readable form. The policies are captured in a machine readable form and are stored to be managed (e.g., modification, deletion, addition). Policies also are staged for use by tools that implement policy enforcement related functions. One way of storing and managing service related security policies is by using a service metadata repository.

Another and broader definition of Security Policy Management can be seen in the context of NAS wide policies that allow or limit access to NAS resources including data and systems.

3.4.6.2   Service Policy Management

Service Policy Management is a function that enables the storing, updating and distribution of service related rules (e.g., message manipulation, exception, performance throttling) established by a governance body. A governance body creates high level policies which get documented in a human readable form. The policies get captured in a machine readable form and get stored to be managed (e.g., modification, deletion, addition). Policies also are staged for use by run-time tools that implement policy enforcement. Service policies are typically stored and managed using service metadata repositories.

3.4.6.3   Service SLA Management

Service SLA Management in the SOA context is a function that enables the storing and updating of service SLAs (e.g., service performance level, availability) established between two organizations (a service-providing entity and a service-consuming entity). Service SLA Management also provides the functionality to collect and review service compliance data collected by run-time tools that implement SLA compliance checking. The end-goal of SLA management in general is to validate whether SLAs are being met. In the broader NAS context SLA management provides the ability to validate whether SLAs associated with NAS systems and services are being met.

3.4.7 Enterprise Service Management

Enterprise Service Management (ESM) as the name implies enables a comprehensive view of services for the purposes of passive and active management of services at run-time. ESM complements traditional system management capabilities and should be viewed in the context of overall management operations of systems and applications.

3.4.7.1 Service Fault Monitoring and Reporting

This function monitors services to determine if a service has a fault or a failure and reports the fault or failure in various forms to operators (e.g., visual alerts). There are a number of functions, both basic (such as "service up or down") and advanced (such as "fault correlation") that come under fault monitoring and reporting.

Fault monitoring and reporting should be considered in the context of traditional management systems which monitor systems, networks, and applications that would be part of SWIM Operations mentioned in Section 2.4.

3.4.7.2 Service Performance Monitoring and Reporting

The ESM function monitors services to determine the level of performance including but not limited to throughput and response time. It also generates threshold based alerts and reports performance based metrics. These metrics are important in generating service scorecards which essentially establish service quality information for consumers and the governance process.

Service performance monitoring and reporting should be considered in the context of traditional management systems which monitor systems, networks, and applications that would be part of SWIM Operations.

3.4.7.3 Service SLA Compliance and Metrics Collection

This functionality supports the monitoring of services to determine if factors specified in SLAs are out of the permitted range, including but not limited to resource utilization, fault behaviors, and performance metrics. Also, relevant metrics such as number or percentage of compliance failures in each of the SLA categories are collected and reported to ESM and/or overall operations portals. A summary of the data is also sent to the governance management system discussed in Section 3.4.6.3 as part of a service scorecard.

3.4.7.4 Service Policy Enforcement and Metrics Collection

This function enforces policies set by the governance process including but not limited to some security policies (e.g., access limitation or control). In addition, data such as the number of times a policy enforcement action was taken when access attempts were made, is collected. Note that there could be policy enforcement functions such as those related to message manipulation or Quality of Service (QoS) supported by entities other than ESM (e.g., ESB) in a SOA environment.

The collected data and related metrics associated with enforcing policies are sent to the governance management system discussed in Sections 3.4.6.2 and 3.4.6.1 .

3.4.7.5 Service Scorecard Generation and Reporting

This function supports the generation and reporting of overall service scorecards for services including but not limited to SLA, policy compliance, performance level, and failure rate as a feedback to the governance process and service quality rating. This rating will provide useful service quality rating for design-time usage (e.g., determination of which services to consume) as well as governance effectiveness validation.

3.4.8 Security Services

This section describes security functionality that is included within the SOA Core Services area.

3.4.8.1 Service Policy Enforcement and Access Management

This function consists of enforcing NAS policies regarding access to services and data resources, including policies based on the requesting entity's identity, organizational role, or other attributes.

3.4.8.2 Service Security Monitoring

This function consists of monitoring NAS services for indication of a security breach or fraudulent use of NAS system resources. Data gathered from this function should be forwarded to a centralized NAS monitoring and analysis facility.

3.4.8.3 Guard Gateway

This function consists of examining data flowing from one enclave to another (including data flowing between NAS and non-NAS) to ensure that data is valid and conforms to expected format and content.

3.5 Technical Infrastructure Services

Technical Infrastructure Services include basic IT and ISS infrastructure that supports SWIM and NAS systems. (Technical Infrastructure Services are provided, in large part, by the "IT and ISS Core" of the NAS net-centric infrastructure described in Section 2.)

The sub-areas that make up the Technical Infrastructure Services are described in the following paragraphs.

3.5.1 Terrestrial Network Communications

IP network transport capabilities needed by SWIM include both Wide Area Network (WAN) and Local Area Network (LAN) capabilities. This includes support for the Internet Protocol Suite (IPS), including not just basic IP service but related services such as Domain Name System (DNS) services, and Network Time Protocol (NTP) services to provide common time reference. In addition, this area includes other IT capabilities such as computing platforms and data storage that are provided as enterprise services.

3.5.2 Boundary Protection

This area includes controls to protect connections and information flows between NAS and non-NAS entities. Boundary Protection is discussed in detail in Section 5.6 .

3.5.3 Computing Platforms

This includes general-purpose computing platforms that may support a variety of NAS computing needs.

3.5.4 SOA Platforms

These are computing platforms that specifically support SWIM Core computing needs.

3.5.5 Data Storage

This includes data storage capabilities (e.g., database engines) that are available for SWIM Core and other NAS needs.

3.5.6 Identity and Key Management Infrastructure

The Identity and Key Management Infrastructure functional area includes capabilities for managing keys and supporting access control in the NAS. These capabilities are described in detail in Section 5.6.

3.5.7 Air/Ground Data Communications

This includes data communications services between ground and aircraft systems.

3.6 Services Provisioning Management

This area includes functions related to preparing applications so that they can be deployed into the NAS to provide (new) services to users and to other applications. The sub-areas that make up Services Provisioning Management are described in the following sections.

3.6.1 Service Integration and Testing

This function consists of assuring that services will operate as intended and not cause problems, before deployment into the operational NAS.

3.6.2 Service Provisioning

This function consists of allocating computing resources to support a service to be deployed into the NAS.

3.6.3 Service Management Support

This function consists of the support for NAS personnel in provisioning NAS services.

3.6.4   Service Diagnostics

This function consists of "second level" support to diagnose problems with services when these problems cannot be immediately corrected in the field.

3.6.5   Training Support

This function consists of training users, operators, and maintainers.

3.7   Data/Network Services Operations Support

This area includes functions related to supporting the operations of the systems and services that provide the functions within the horizontal bars shown in Figure 3-1.

3.7.1   Database Administrative Services

This function consists of supporting the operation of the Data Storage function within Technical Infrastructure Services.

3.7.2   System and Service Management

This function consists of supporting the operation of Interaction Services, Support Services, and SOA Core Services. (Note that support for the systems and services that provide specific functions within the Mission Services area is broken out separately as the "Systems and Services Management" function within that area.)

3.7.3   Network Support Services

This function consists of supporting the operation of the systems and equipment that provide the Terrestrial Network Communications and Air/Ground Data Communications functions within the Technical Infrastructure Services area. This includes monitoring and management of the network, as well as administration of ancillary functions necessary to the smooth functioning of the network, such as allocating host names and addresses, and managing the system that translates host names to network addresses.

3.7.4   Identity and Key Management Administration

This function consists of administering the Identity and Key Management Infrastructure within the Technical Infrastructure Services area.

3.7.5   Help Desk

This function consists of coordinating and responding to requests for help from operators and users throughout the NAS.

3.7.6   Incident Detection and Response

This function consists of monitoring, analyzing, and correlating incident detection sensor data from throughout the NAS, as well as reporting and coordinating response activities when an incident does occur.

3.7.7   Certified Software Management

This function consists of providing a central source of approved software for use in the NAS, including the ability to ensure the integrity of this software.

4 SWIM Technical Architecture

4.1 SWIM SOA Standards Approach

The SWIM program will, in collaboration with the SIPs, define standards to be used in each segment. The initial standards for SWIM Segment 1 were defined in the Segment 1 SWIM Technical Overview document. SWIM Segment 2 standards will be identified at a future time.

4.1.1 Accommodating Change in SWIM Architecture

Standards in the SOA environment are evolving rapidly, and should be expected to change, perhaps dramatically, between SWIM segments. To accommodate the rapid evolution of standards, this SWIM architecture encourages the separation of mission logic components, which implement Air Traffic Management (ATM) services, from IT components, which implement standards-based core services. For example, the Service Container software component is intended to allow IT software components to be replaced as necessary to adapt to changing standards, with minimal impact on software that implements the ATM logic to provide access to NAS system services.

4.1.2 Approach to Combining Web Service Standards and non-Web Service Standards

SOA is a general concept or paradigm for system-of-systems structure. SOA can be implemented with a variety of technologies and standards. SWIM Segment 1 emphasized use of Web Services standards. SWIM Segment 2 will likely be the same. At the time of this writing, Web Services standards continue to be promising and are widely used for implementing SOA in a way that improves interoperability and flexibility.

The intent of the SWIM architecture is to allow other standards besides Web Services standards to be used when necessary, while retaining general SOA principles. To accomplish this, SWIM Registry components should be capable of including information on services that are provided using a variety of different technologies and standards. Similarly, SWIM Enterprise Service Management and Service Security components should be engineered, to the extent practical, to allow a variety of different technologies and standards to be managed and secured, respectively. This should be addressed during the requirements definition and design phases for the components that implement these functions.

4.2 SWIM Standards for Segment 2

The SWIM Standards for Segment 2 will be defined prior to the start of Segment 2 design efforts.

5 Architecture Analysis and Options for SOA Core Service Areas

In this section we present the SWIM Segment 2 architecture in terms of the major components that will be needed and how these components can be arranged and interconnected to provide the functions discussed in Section 3. Hardware and software components are identified in general high-level terms, not intended to specify any specific product or physical implementation. The components are grouped into the following major areas:

- Enterprise Messaging Bus

- Web Hosting

- Collaboration

- Interface Management (Registry)

- Enterprise Service Management (ESM)

- Security

Each of these areas of the architecture is described in some detail in the following sections. For each area, we define the scope of the area and the considerations which drive the Segment 2 architecture. We then analyze these drivers to come up with two architecture options for Segment 2 (not including the federated option to be used in Segment 1).

Figure 5-1 provides a high level overview of the SWIM architecture, providing a context in which the architecture components will be described further in the following sections. As shown in the figure, Mission Services, which provide access to the essential information and functionality needed for NAS operations, are deployed and operated within end systems that are the primary responsibility of specific SIPs. The figure also shows Support Services and Interaction Services, which distribute, aggregate, and transform NAS information and make it available to users over the network. The figure shows that Support Services and Interaction Services are deployed and operated within a SWIM Core environment, supported by a SWIM Operations capability including ESM.

Note that the representation of a SIP environment as a single block in Figure 5-1 is not intended to imply that a SIP system is located within a single physical facility; some SIP systems may span multiple locations across the entire NAS, and multiple different SIP systems may be located within the same physical facility.

The discussion in this section assumes that the SWIM Core consists of new infrastructure provided by the SWIM Program, and presents different architectural options for this infrastructure. However, at the time of this writing, a final decision has not been made on whether SWIM Segment 2 will include the creation of such a SWIM Core. Section 6 will include a discussion of the option of continuing the federated approach.
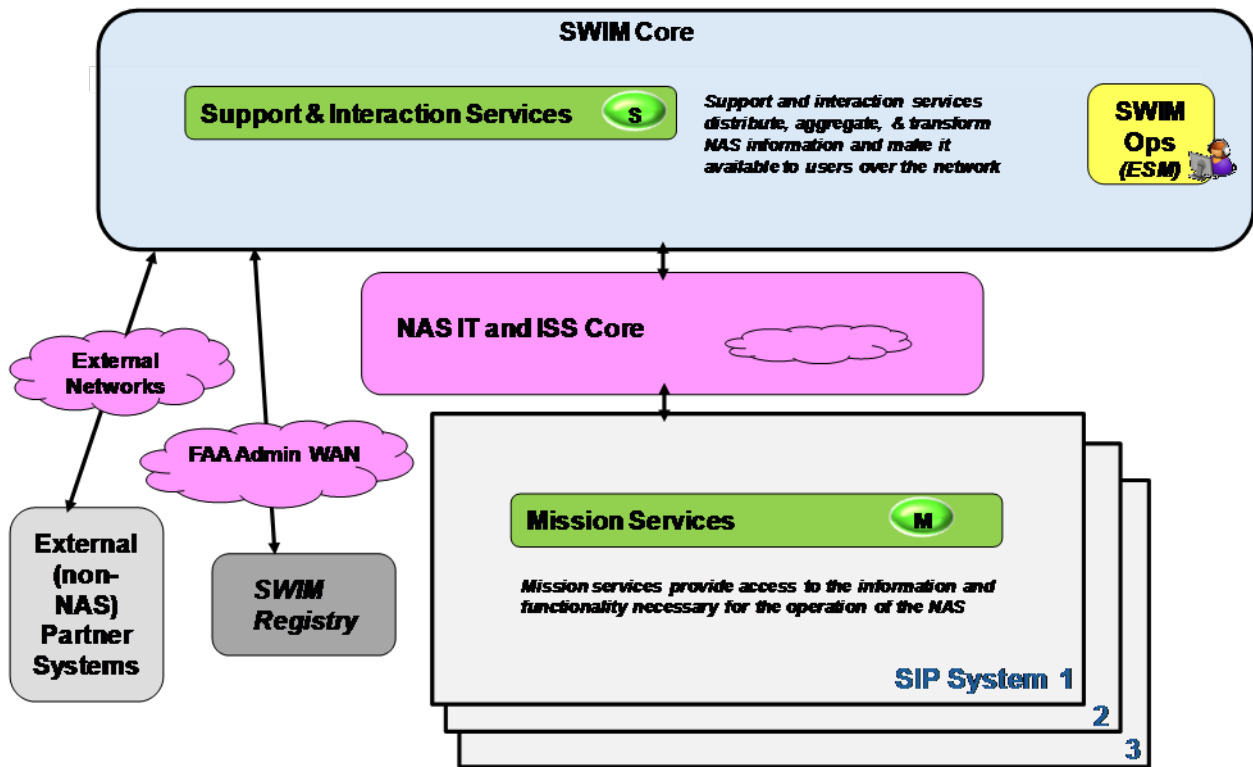
Figure 5-1. Overview of SWIM Segment 2 Architecture

5.1 Enterprise Messaging Bus

5.1.1 Scope

The Enterprise Messaging Bus (EMB) is a set of components that allow NAS systems and services to interoperate by connecting them together in a loosely coupled manner. This is shown in the NextGen 2025 System Interface Definition diagram (FAA, NextGen 2025 System Interface Description SV-1P March 2009), which depicts NAS services using a ubiquitous EMB. The Enterprise Messaging Bus capabilities primarily support two main areas of the SWIM functional architecture: Messaging Services and Service Construction Capability. This section describes different components (primarily software tools and products) that can be used to create an EMB capability in SWIM Segment 2.

5.1.2 Drivers

There are a number of drivers that contribute to messaging architecture options which are described below.

5.1.2.1 Next-Generation Air Transportation System Implementation Plan (NGIP)

The NGIP is a plan issued by FAA for operational and system improvements in the NAS for the midterm (2012-2018). The analysis of NGIP operational capabilities which is referred to in this

document is a study done by MITRE/CAASD in the area of Air Traffic Operations (ATO) (Boan and others September 2008). NGIP Capabilities such as *Flexible Airspace Management and Initial Conflict Resolution Advisories* were examined for data flows between producers and consumers of information in an operational context (Prabhu and Thomson March 2009).

5.1.2.2   Industry Best Practices and Available Technology

To provide the EMB capability, industry has created a variety of products and, just as important, architectural approaches for utilizing these products. One of the most prominent architectural approaches is termed SOA. The analysis and options discussed below are based on these emerging technologies and the general SOA approach.

5.1.2.3   SWIM Segment 1 Architecture

The scope of sharing SOA infrastructure by SIPs in Segment 1 is limited in that the underlying SIP SOA infrastructure (e.g., messaging, security, service management) continues to remain distributed. However, the sharing of SOA services infrastructure provides a potential for cost savings and operational efficiencies. This drives the consideration of a SOA messaging backbone that can facilitate the sharing of SOA infrastructure across the NAS.

5.1.3   Analysis

This section describes how emerging SOA technologies may be used in SWIM Segment 2, consistent with a SOA approach, to create an EMB that can provide Messaging, Service Construction Capability, and other functions needed in SWIM Segment 2.

5.1.3.1   Message Brokers

Shared messaging services functionality in the SWIM Segment 2 architecture can be supported with a widely available and mature messaging infrastructure technology called Message-Oriented-Middleware (MOM). Examples of MOM products are: MSMQ, MQSeries, and ActiveMQ.

MOM represents a broad range of products that are not fully standardized and are not always interoperable. However, all major MOM products support a standard Application Programming Interface (API) known as JMS. MOM products using the JMS standard include support for the following messaging functions included in the SWIM functional architecture shown in Figure 3-1:

- Publish/Subscribe and point-to-point messaging
- Reliable Messaging
- Message Routing, and
- Message Transport

(Mediation is covered in Section 5.1.3.5 and Messaging Security (integrity and confidentiality) is covered in Section 5.1.3.9)

5.1.3.2   Use of Message Brokers in SWIM Segment 2

All of the options considered in this architecture assume that MOM Message Brokers will be deployed in the SWIM Core to provide the backplane in a NAS wide messaging exchange. SWIM Core Message brokers will provide de-coupling between the SIP sender and the SIP receiver where both are clients of the SWIM Core Message Broker. The connection dependencies between SIP messaging systems will be replaced by connections between SIP systems and SWIM Message Brokers, reducing operational support complexities. This section describes how Message Brokers can be used in the SWIM Segment 2 architecture.

5.1.3.2.1   Using Brokers to Provide a High-Availability Messaging Infrastructure

In order to meet the availability and performance requirements of Mission and Support Services in SWIM Segment 2 and beyond, the SWIM Core messaging infrastructure will likely need to be designed to provide high-availability. Such a design would include features such as reliable hardware, failover clustering, replicated message stores, crash recovery, fast startup, etc., and the cost of incorporating such features may not be trivial. Designing SWIM Core message brokers where re-use or sharing of such a highly available messaging system can take place can result in long-term cost saving. A highly available SWIM Core messaging infrastructure would include support for load balancing, failover configurations and flexible deployment options, as described further below.

To prevent the SWIM Core message broker from becoming a single point of failure, the SWIM Segment 2 architecture envisions providing multiple SWIM Core message brokers in a *cluster* which can provide failover in case of broker failure. A common model of clustering is illustrated in Figure 5-2. In Figure 5-2, the sender is connected to one of the message brokers in a cluster and has a static failover list with addresses of the three message brokers in the cluster. In case of failure of any of the SWIM message brokers, its clients will auto-connect to another active broker in the cluster. The discovery of other brokers can either be static (a hardcoded mechanism of failover to a static list of broker instances) or dynamic (using a multicast discovery agent). The *store and forward* capability of the active broker will ensure that the message gets delivered to the SWIM message broker to which the receiver is connected to in the cluster.

5-4
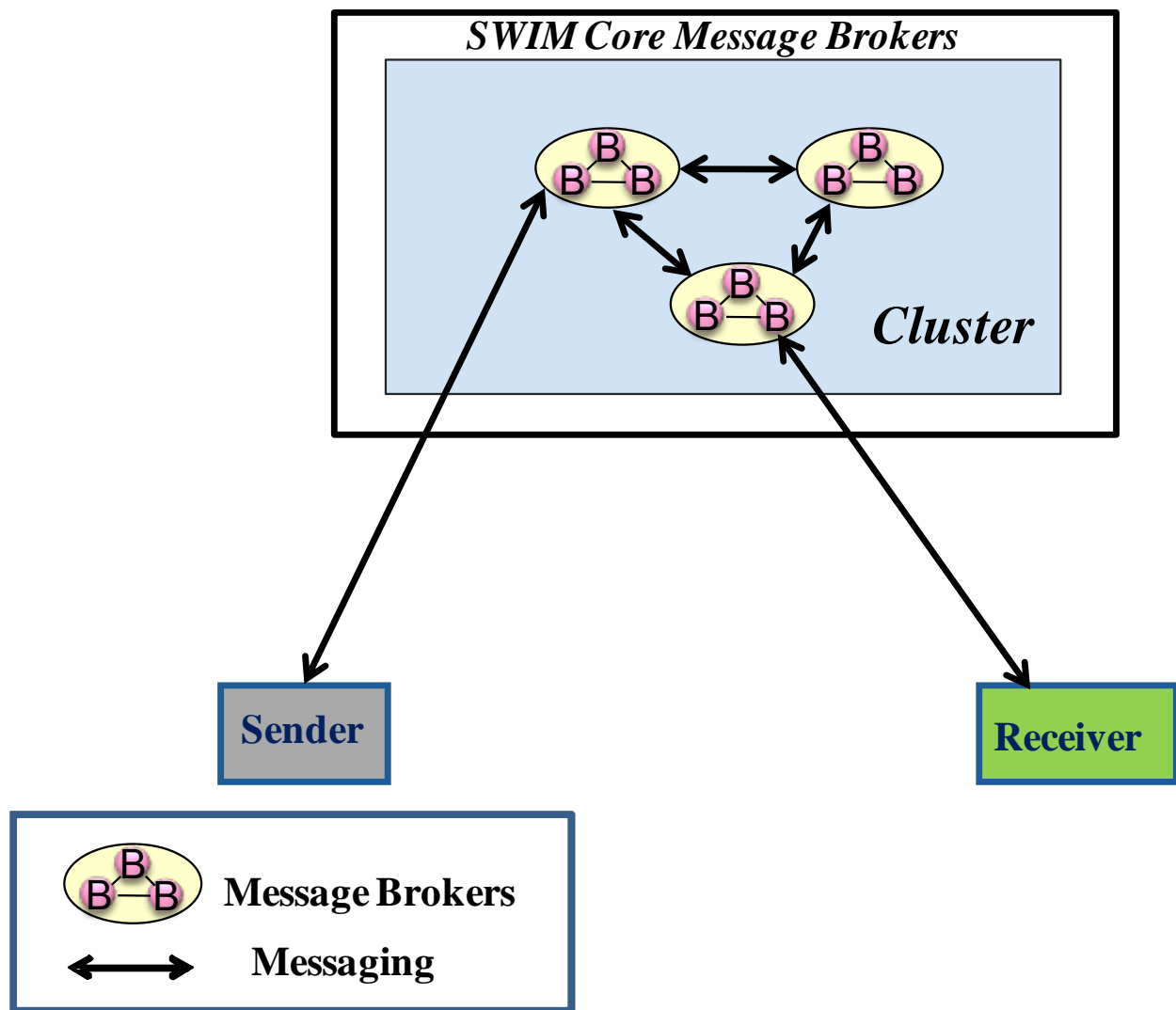
Figure 5-2. Cluster of SWIM Core Message Brokers

Different vendors have various schemes and configurations for providing clustering in Message Brokers.

5.1.3.2.2   Hierarchical Messaging with SIP-deployed Brokers

If all the messaging is consolidated to only SWIM Core message brokers then it may become complex to configure and manage all the connections with message producers and consumers within SIP domains. To avoid this issue, a hierarchical network of brokers can be deployed where central SWIM message brokers can be connected to SIP-deployed brokers. To illustrate the concept, in Figure 5-3 below, SIP1 and SIP2 have deployed their own messaging infrastructures for messaging within the SIP domains. For messaging between SIP1 and SIP2 (between different NAS systems), the local SIP1 producer sends messages to its SIP1 message broker, which sends messages to the SWIM Core message broker cluster, to be forwarded to the

SIP2 message broker. The SWIM Core message broker thereby provides routing between SIP1 and SIP2. The advantage of this hierarchical broker network is that the maintenance of local SIP messaging connections on SWIM Core message brokers is reduced, and SIPs can optimize and administer their messaging infrastructures for their own needs and environment.
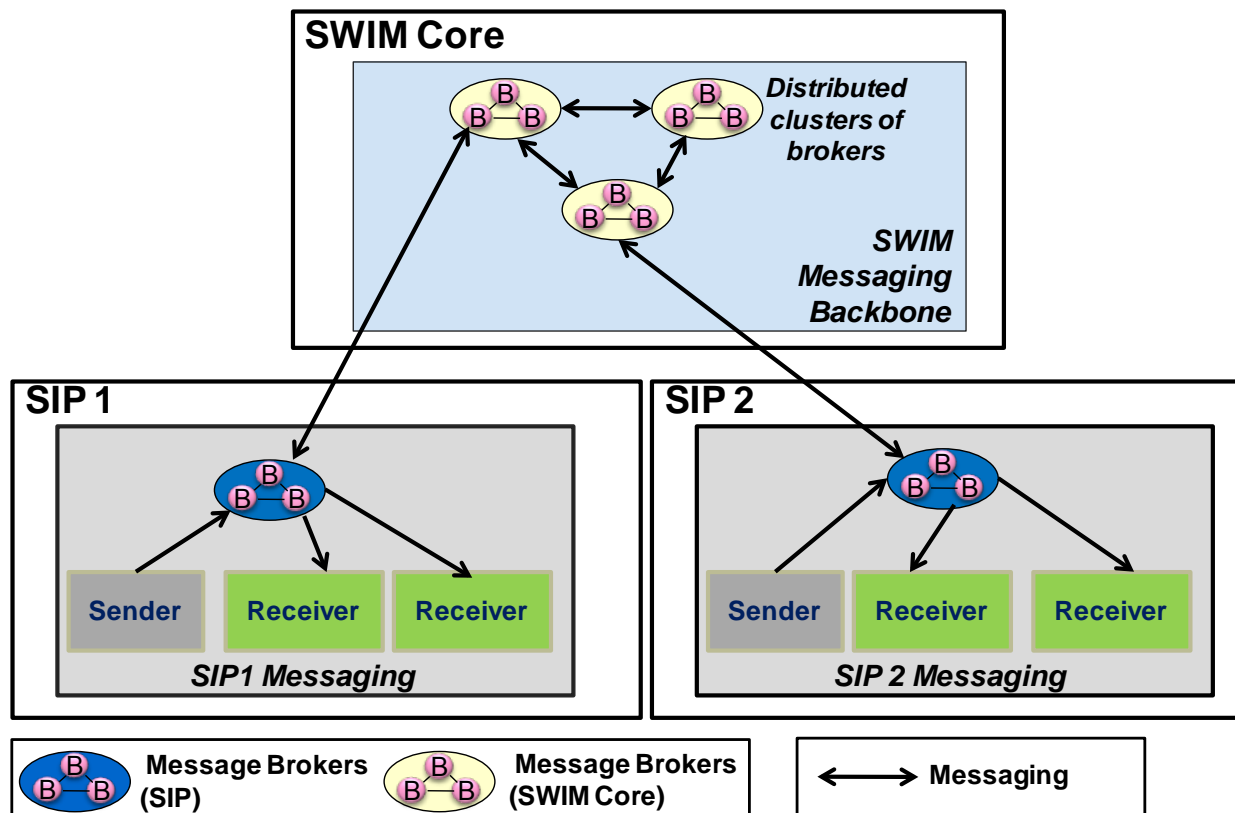
Figure 5-3. Network of SWIM Core and SIP Message Brokers

5.1.3.2.3 Physical Messaging Architecture Considerations

The simplified concept of hierarchy of brokers shown in Figure 5-3 to support a messaging backbone in the NAS has to consider the challenge of not only geographically separate NAS physical facilities and their connectivity but also the boundaries of SIP program control. A notional physical deployment of SWIM Core message brokers and SIP brokers between multiple facilities is shown in Figure 5-4 and Figure 5-5.

Figure 5-4 shows an example of how SIP-deployed message brokers may be interconnected in SWIM Segment 1. The figure shows that SIP1 and SIP2 have deployed their own separate distributed messaging capabilities that span multiple facilities, whereas SIP3 and SIP4 have messaging capabilities that exist within specific facilities. In order for these SIPs to share information, they interconnect their messaging infrastructures both within and between facilities, as shown in the example. Note that these interconnections cross many different domain boundaries, and bilateral agreements must be put in place for these interfaces, including cross-domain security controls.
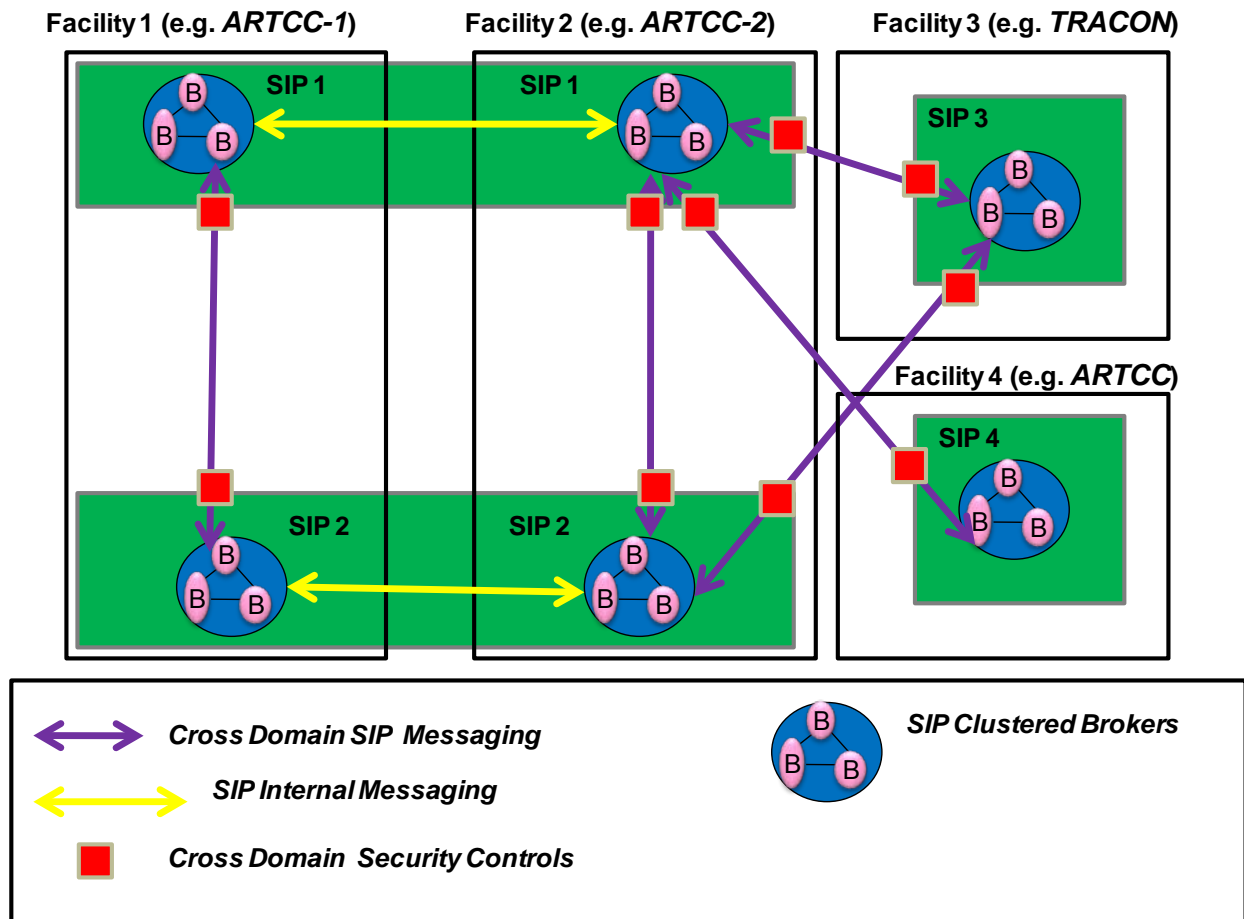
Figure 5-4. Example Physical Messaging Architecture (Segment 1)
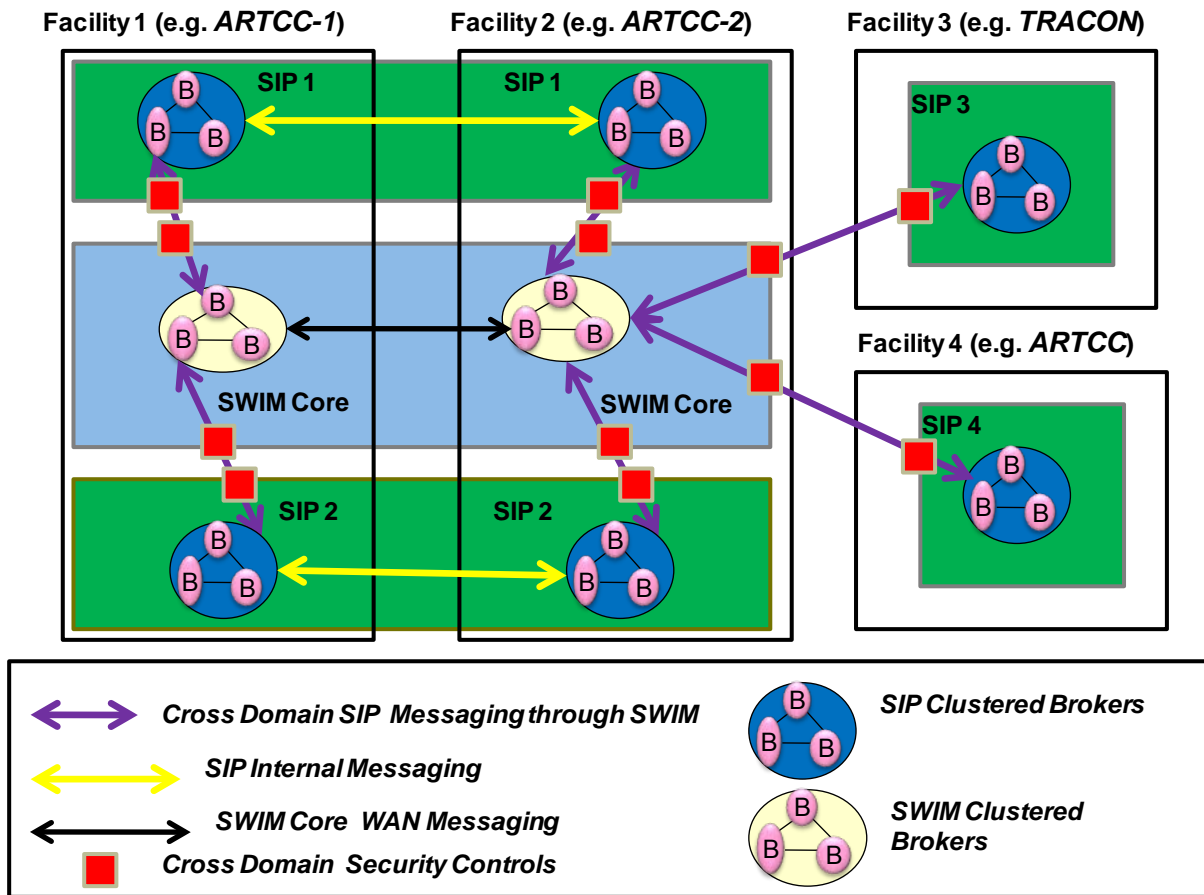
Figure 5-5. Example Physical Messaging Architecture (Segment 2)

In contrast, Figure 5-5, shows an example of how a distributed SWIM Core messaging backbone may be added in Segment 2. This architecture allows SIPs to continue to administer their own backbones for SIP-internal messaging, but the use of the SWIM Core messaging backbone provides for security and policy controls to be applied uniformly for messaging between the SIPs. In Figure 5-5 we show that the interconnections between different SIP messaging backbones have been replaced with interconnections between the SIP backbones and the SWIM core. Specifying a uniform messaging interface and security controls for connecting SIPs to the SWIM core reduces the potential number of unique bilateral interfaces. With this approach, each SIP will need to support only one cross-domain SWIM messaging interface, rather than each SIP needing a messaging interface with every other SIP.

As shown in the example, the SWIM Core messaging backbone may span multiple NAS facilities, but may not have a point of presence in all facilities. During the Segment 2 design phase, the actual physical locations of SWIM message brokers must be determined based on an analysis of messaging needs for capacity, latency, availability, and so on.

5-8

5.1.3.2.4   Security

Authentication, authorization, and messaging security can be supported by a variety of mechanisms, including Java security APIs, username/password combination, or digital certificates (see Section 5.1.3.9).

5.1.3.2.5   Message Bridges

Since there is no requirement in JMS-based brokers to have wire-level interoperability, SWIM message brokers will interoperate with SIP provided message bridges or adapters for SIP brokers from a different vendor.

5.1.3.3   Segment 1 Transition to Message Broker based Messaging

In this section, we consider how the existing infrastructure being deployed by the SIPs in Segment 1 will interoperate with, or transition to, the Segment 2 messaging infrastructure describe in this architecture.

Some examples of transition from Segment 1 to Segment 2 SWIM Core Message Brokers are depicted in Figure 5-6 below.
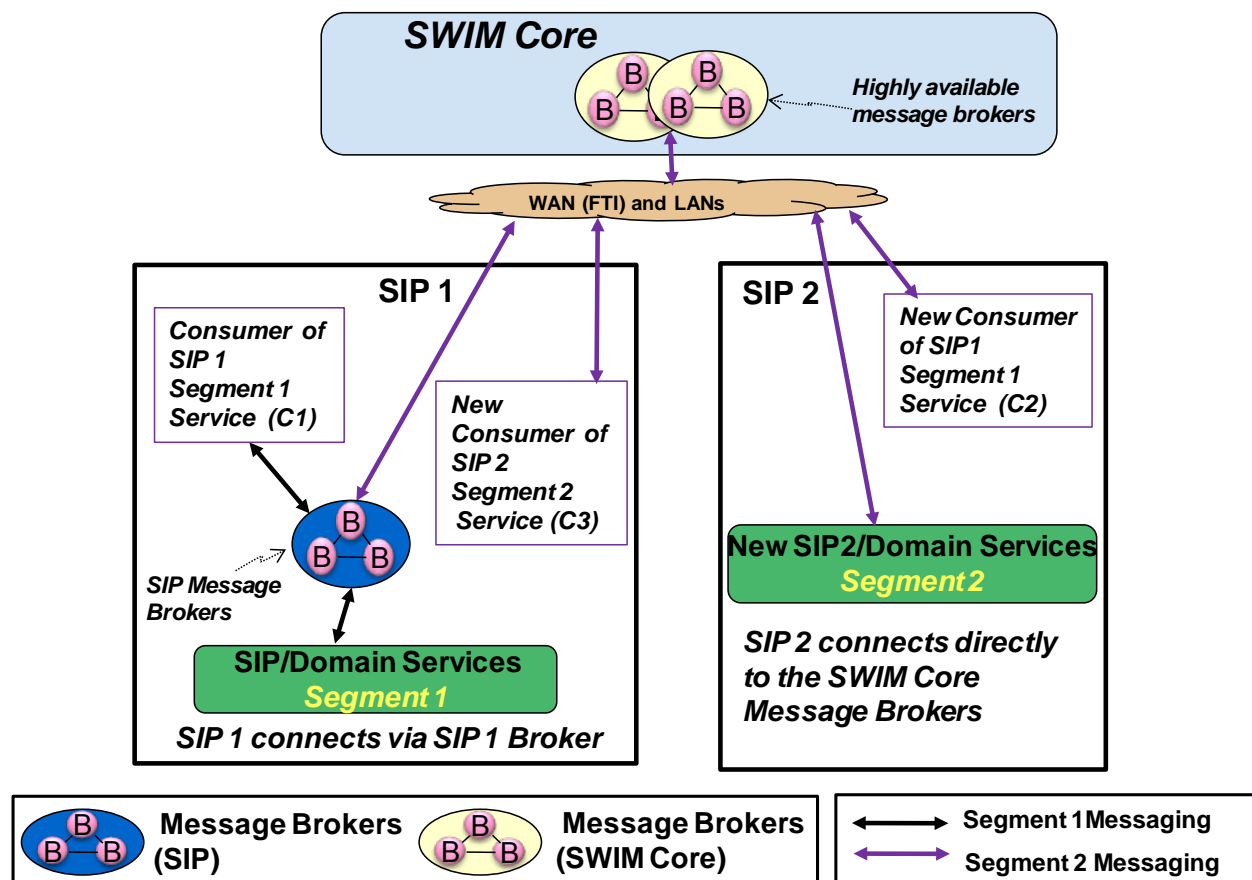
Figure 5-6. Transition Paths for Segment 1 Messaging to Segment 2 Message Brokers

Case 1: New Consumers of SIP Segment 1 Service in Segment 2

This case illustrates how new Segment 2 SIPs, that have not already deployed their own messaging infrastructure, can use the SWIM Core to consume services that were developed in Segment 1 using SIP-provided messaging infrastructure. As illustrated in Figure 5-6:

- SIP 1 is a service provider that has deployed its own message broker in Segment 1. The service is provided by sending messages from a system within the SIP 1 domain to the SIP 1 broker.

- C1 is an existing consumer of SIP 1 Segment 1 service. C1 consumes messages related to SIP 1 service from SIP 1 message broker.

- In Segment 2, the SIP 1 message broker will be connected to SWIM Core message broker, using a bridge if required to overcome product differences.

- C2 is a new consumer of the SIP 1 Segment 1 services over the network. C2 consumes the SIP 1 Segment 1 service by connecting to the SWIM Core.

Case 2: New Segment 2 Service Providers

In this case, new SIPs in Segment 2 provide services by connecting directly to the SWIM Core message brokers. One or more message brokers in the SWIM Core may be configured to provide for SIP 2 messaging destinations. As illustrated in Figure 5-6:

- SIP 2 is a new Segment 2 service provider. SIP 2 enables its service by connecting to SWIM Core message brokers.

- C3 is a consumer of SIP 2 service. C3 consumes SIP 2 Segment 2 service by connecting to SWIM Core message brokers. (In this example, C3 is a new capability added to SIP1 in the Segment 2 timeframe.)

5.1.3.4   Web Services Framework

A Web Services Framework (WSF) consists of software development tools that allow creation of applications that can send and receive SOAP messages over a variety of transports, including JMS and HTTP, in accordance with the WS-* family of industry standards that have been adopted by SWIM. One example of a WSF is *Apache CXF* (*FUSE Services Framework)*. SOAP over HTTP has industry wide adoption because it has no binary dependencies between the sender and the receiver of message data. There is additional meta-data in the header in the SOAP message that will be used for adding security based information (WS-Security) and further will make messaging and security integrations seamless across NAS enterprise boundaries. Reliable Messaging in the SWIM Core with WSFs can be supported by the standard WS-Reliable Messaging [WS-RM] protocol. The WS-RM protocol provides reliable SOAP message exchange in distributed applications, in the presence of communication failures. SOAP on JMS transport can also be used because of the *reliability* and *durability* of JMS messaging.

The use of message brokers in the SWIM Core, as described above, provides a messaging backbone, but additional components are needed for web services construction using HTTP and applications hosting capability to be supported in the SWIM Core. One way to provide this is to

5-10

use Web Services Frameworks (WSFs) to allow web services to be implemented and deployed to computing platforms provided in the SWIM Core.

WSFs deployed in different geographic locations in the NAS, among different NAS service providers can result in distributed mission services. Interaction between programs based on WSF will isolate the NAS program mission/business logic from the distributed communication logic and its messaging formats. The NAS mission service or specific business function of a NAS program is described by a Web Services Definition Language (WSDL) contract, machine readable and addressable; message exchanges with specific functions can be invoked by another NAS program for consumption.

Services in the SWIM Core can be built using WSF using either SOAP or the REST (Representational State Transfer) architectural style. The REST style of messaging sends XML payload directly over HTTP, and service operations are passed as parameters in the Uniform Resource Locator (URL), which is the target of the operation or the "resource". *Presentation* or *Interaction Services* which are consumed by browser type technologies within the NAS are a good candidate to be considered for REST architecture. REST-based Services can be deployed in the SWIM Core by using WSF's (e.g., Apache CXF) and Java API for RESTful Web Services (JAX-RS). Since REST does not support WS-Security it is not appropriate for applications where a standard security mechanism is needed; it may be appropriate for NAS internal services where lightweight (non-secured) service architecture is needed.

5.1.3.5 Mediation Platforms

In messaging between NAS applications, there may not be agreement on the protocols or formats of the message data being exchanged. Components which support message mediation in the form of message translation or message transformation may be needed.

Transformations can be supported in different layers. Transport level mediation refers moving data across different protocols without affecting the message content. Transport level adapters, such as those used in the FUSE Mediation Router, support mediation between different transports in the SWIM Core.

Data Representation mediation occurs when the data that is being transported has to be transformed to another XML representation to be consumed by the receiving application. XML transformation can be achieved by use of eXtensible Stylesheet Language Transformations (XSLT). Enterprise Integration Patterns (Gregor Hophe October 2003) covers the various 65 design patterns used for mediation. Products such as FUSE Mediation Routers (Camel) implement these design patterns.

A notional example is a SWIM Core based weather data notification system shown in Figure 5-7 where combined use of reliable request/response, mediation and broker based messaging in SWIM Core illustrates service construction. Weather Data may be consumed by different services in the NAS. A SWIM Message Broker can become a mechanism in providing weather notifications to SIP consumers which subscribe to SWIM Brokers for receiving weather data. A Web Service Requester/Client using WSF in the SWIM Core makes a request in a SOAP

message over HTTP using WS-RM to a Weather Data Web Service Provider (using WSF) for weather data.
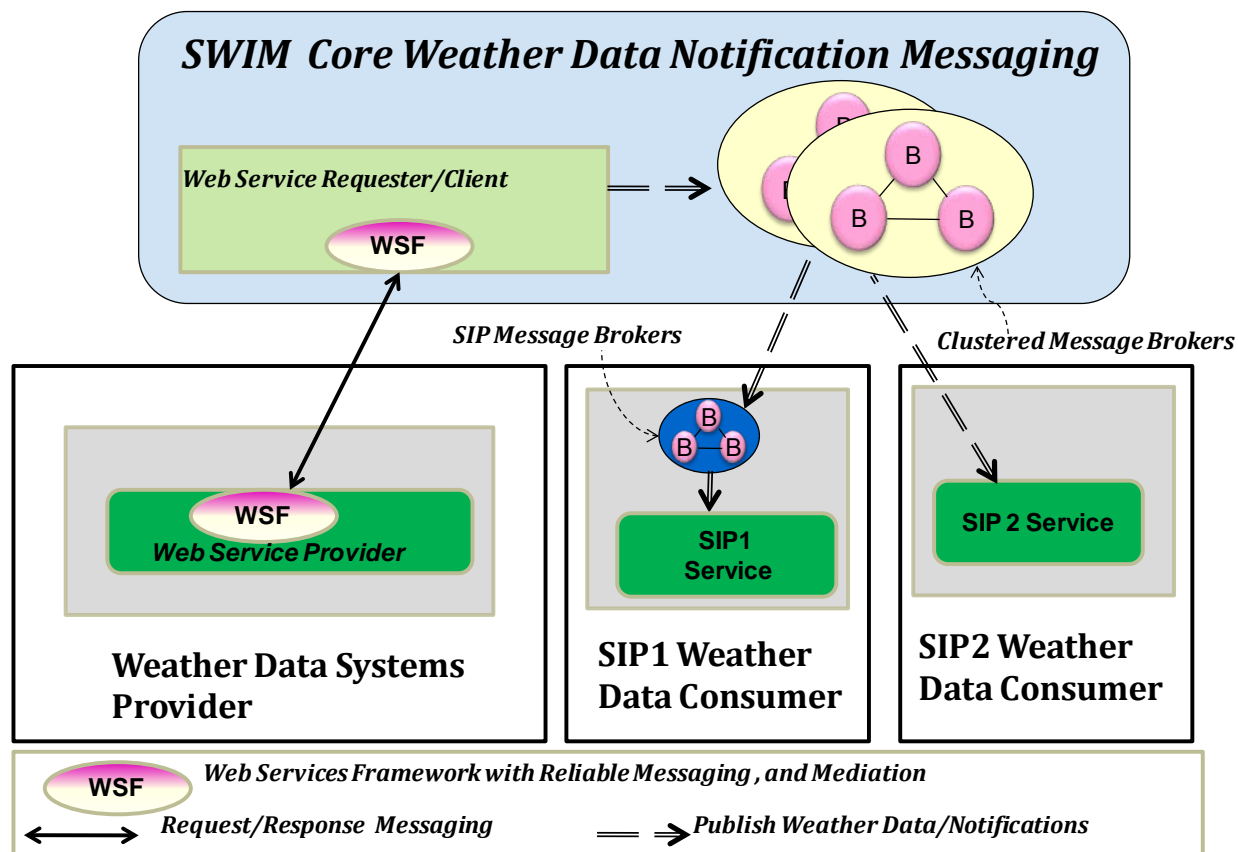
Figure 5-7. Message Brokers, Web Services and Mediation Platform used for Weather Data Notifications in SWIM Core *(Notional)*

In Figure 5-7, the Web Service Requester/Client reliably receives the weather data in response to its web service request to the Weather Data Systems Provider. The received data in the Client has to be sent to the clustered SWIM message brokers where the consumers of the weather data have registered for notifications. The weather data requester/Client will add *mediation rules* logic in the form of *transport and data representation* transformation by using a *mediation router* to convert to JMS messaging of the SWIM Core message brokers and weather data formats as used by other SIP consumers. The transformed weather data notification will be sent to the SWIM Core message brokers. SIP1 and SIP2 are the weather data consumers and use weather data to create SIP based Services as denoted by *SIP1 Service* and *SIP2 Service* above. Varied messaging consumption by different SIPs is illustrated by SIP1 and SIP2. SIP1 service receives notification of weather data from its local SIP message broker which is connected to SWIM Core message brokers. SIP2 has directly registered as a consumer with the SWIM Core message brokers and receives weather data notifications directly.

The notional weather data notification mechanism (shown in Figure 5-7) could support messaging and service construction of *Weather Data Management* (as in SV-4) in the SWIM

5-12

Core by deploying applications using components like message brokers, WSFs and mediation routers.

5.1.3.6   Enterprise Service Bus Products

Enterprise Service Bus (ESB) products can be used to provide a backplane for distributed messaging and service integration. Examples of ESB products include *JBoss ESB, Open-ESB, Sonic ESB, IBM Websphere ESB, TIBCO Business Works, FUSE ESB, and Apache ServiceMix*.

ESB products can be used in the SWIM Core to provide the following higher level functions:

Messaging Core: ESB products often include a core messaging backbone, capable of asynchronously transporting messages reliably. This messaging core could be a generic messaging engine, or a proprietary MOM, or a MOM based on JMS as described in Section 5.1.3.1. or any combination of these. ESB products also support a variety of different transports, in particular SOAP and HTTP.

Message Routing: Distributed integration can be achieved by routing messages between different services. A message is sent to its destination either through hard-wired (static) logic or dynamically based on content. *Content Based routing (CBR)* decides the destination of the message using the properties of the message itself. The method of specifying the branches of routing and the details of how the routing of the messages is applied vary with vendor implementations. The main discriminating aspect of the ESB is that the meta-data related to the routing of the message and the routing rules are not centralized in a central rules engine (e.g., broker) but are distributed, and are evaluated in the service container in which the message is being processed. CBR is a service in an ESB and holds its own instructions in its own container, without referring to any external centralized rule engine for the whole ESB.

Protocol Mediation and Message Transformation: An incoming message can be transformed at transport level (*HTTP to JMS Messaging like ActiveMQ*) or message content can be transformed in its data representation (e.g., XML format to a message data format that can be written to a data base).

ESB Endpoints: Each component or application in the ESB is an endpoint and is integrated with other endpoints in a consistent way. The common messaging core is used for communicating consistently with the other endpoints.

Service location transparency in an ESB allows a service client to use a logical service endpoint, and the actual physical service endpoints remain hidden. It allows for flexibility in managing NAS services, where modifying physical service endpoints are possible without recompiling NAS service clients.

To achieve high availability of an ESB architecture in the SWIM Core, deployment of a network of active ESB containers connected together in a cluster is needed. The members of the cluster communicate and load balance by different message flows between ESB containers using vendor specific implementations. Persistent messaging in ESB products provides fault tolerance for failed endpoints, where the messages are routed to active ESB containers in an ESB cluster.

SWIM Core Weather Data Notification with Enterprise Service Bus product (ESB)

Web Service Requester/Client

ESB

ESB

SIP Message Brokers

Clustered ESB

WSF
Web Service Provider

SIP1
Service

SIP 2 Service

Weather Data Systems Provider

SIP1 Weather Data Consumer

SIP2 Weather Data Consumer

WSF — *Web Services Framework with Reliable Messaging*

Request/Response Messaging ⟷   ══▶

Figure 5-8 Basic ESB used for Weather Data Notifications in SWIM Core *(Notional)*

ESB products like an *Apache ServiceMix (FUSE ESB)* in the SWIM Core can be used to provide the ESB architecture pattern functionality and have an extensible architecture to allow different components to be added to provide additional functionality if needed. In the notional example of notification of weather data from the SWIM Core which was described in Section 5.1.3.4, the distributed components shown in Figure 5-7 can be replaced with an ESB product cluster as shown in Figure 5-8. The cluster made of ESB products shown in Figure 5-8 provides similar functionality of messaging, transformations, and notification as was discussed in Section 5.1.3.4. Additionally, ESB in the SWIM Core can provide a service proxy for SIP services on a different transport than that of the SIP deployed services.

ESB products which support the Java Business Integration (JBI) specification have an architecture where services and the bindings (transport) are separated into components. ESB products may also use Open Services Gateway initiative (OSGi) specification which standardizes the deployment model and manages the components dynamically (e.g., stop, start services without stopping the ESB). These standards are not supported by all ESB vendors, (e.g., FUSE ESB 3.x supports JBI spec and FUSE ESB 4.x supports OSGi and JBI as well). Using an ESB product in the SWIM Core that supports these standards will operationally create a consistent deployment model which eases maintenance.

5.1.3.7   Use of Enterprise Service Bus in the SWIM Core

In general, ESB products provide a higher degree of integration that is intended to overcome some limitations of the product categories that have been discussed previously (message brokers, WSFs, and mediation platforms). The main concern with using message brokers, WSFs, and mediation platforms is that there is huge variation possible in how these products are used to create Support Services. As the variation in the use of these products increases, the expertise required for operationally maintaining the SWIM Core becomes greater. The issue of inconsistent integration points, as a result of using distributed and varied components, is addressed by using ESB products. In particular ESB products support standards such as JBI. These standards, which are still emerging and maturing, promote more uniform models of service deployment and integration. Selection of a single ESB product suite for the SWIM Core will reduce the technical expertise needed to configure, operate, and maintain the SWIM Core, as compared to the mix of message broker, WSF, and mediation platforms.

Table 5-1 summarizes some of the advantages and disadvantages of ESB products. Caution must be exercised in selecting an ESB because products may be built internally with a proprietary implementation which may inhibit how well it integrates with other existing SIP components. It is desirable to require a standards based ESB product in the SWIM Core which can then be integrated with other standards based modules.

Table 5-1. Basic ESB Advantages and Disadvantages

Advantages	Disadvantages
• Messaging core and distributed service integration • Pluggable, extensible with components for adding custom functionality	• Not all ESB products are standardized • Standards are still maturing

5.1.3.8   Advanced ESB Use

Service construction needs to be flexible, re-usable and use the *leave-and-layer* approach of continuing to leave the existing IT infrastructure in place while developing new service capabilities related to mission needs. Development of *Support Services* such as *Content Discovery, Flow Data Management*, and *Weather Data Management* may require advanced service construction capabilities, which are provided within ESB products that have capabilities such as Orchestration and Service Composition.

5.1.3.8.1   Use of ESB for Service Composition

Service composition consists of combining functions and services of multiple participants into a composite service. Composing higher-grained services from fine-grained services is the most common model of use.

5-15
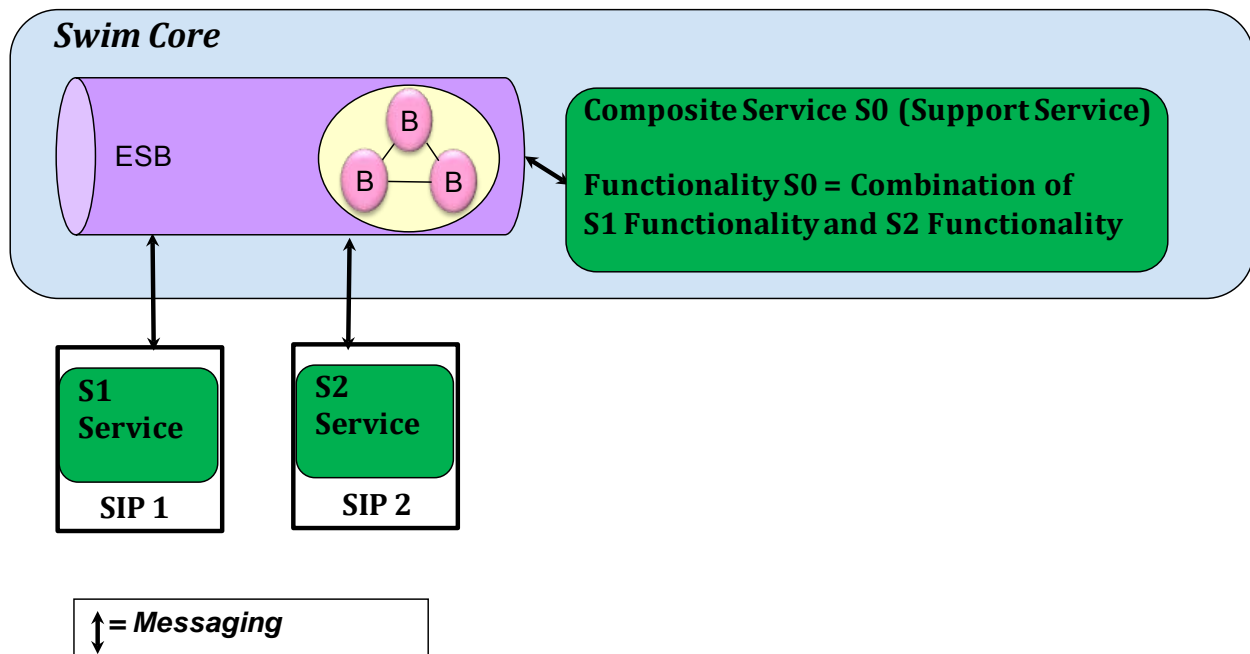
Figure 5-9. Service Composition using an ESB product

As an example of Service Composition in the NAS, consider the problem of creating service that provides information on the status of a certain sector of airspace. This service would provide a combined view of airspace information that contains temporal as well as static information of sector definitions that do not change frequently. Congestion, traffic management initiatives, special airspace usage schedules, runway closures, airspace constraints and weather all modify the current airspace information. Most services that can provide information on any aspect of the airspace may have to consider ingesting dynamic and static data from different sources and combining it to create the most recent view of the airspace. In these cases, composition of services may apply, where a number of services are invoked to provide the most recent data with respect to a domain and then combined with other types of data from another service (e.g., sector data which is static) and provide a mission function (e.g., traffic in a sector of an airspace). Figure 5-9 shows composite service S0 which combines responses from invocation to SIP1 service S1 and SIP 2 service S2 to provide service S0. In providing the service S0, the integration capability of the ESB with respect to mediation of message and transport may be used to combine the data received from S1 and S2 if differences in message and transport protocols exist. Other additional components like databases may be used to provide persistence if needed.

If the requirements are of a data-centric nature, as in handling complex data transformations in large volume of messages, then an ESB alone is the choice. If the requirements include complex logic, as in interactions between stateful mission processes, then an ESB product with additional orchestration engine processing may have to be used, as discussed below.

5.1.3.8.2 Service Orchestration

An orchestration service provides new functionality by coordinating other services and maintaining state information on the enterprise service bus over a span of time.

Many mission/business level functions are of long duration and are stateful (e.g., filing a flight plan and receiving clearance for flight is a stateful business process). For a long duration stateful service interaction, an orchestration service can be chosen, when external events with pauses and resumes that are separated by time have to be processed. The events in the long running process can be a person clicking an Approve button or the process waiting for a particular type of message to arrive.
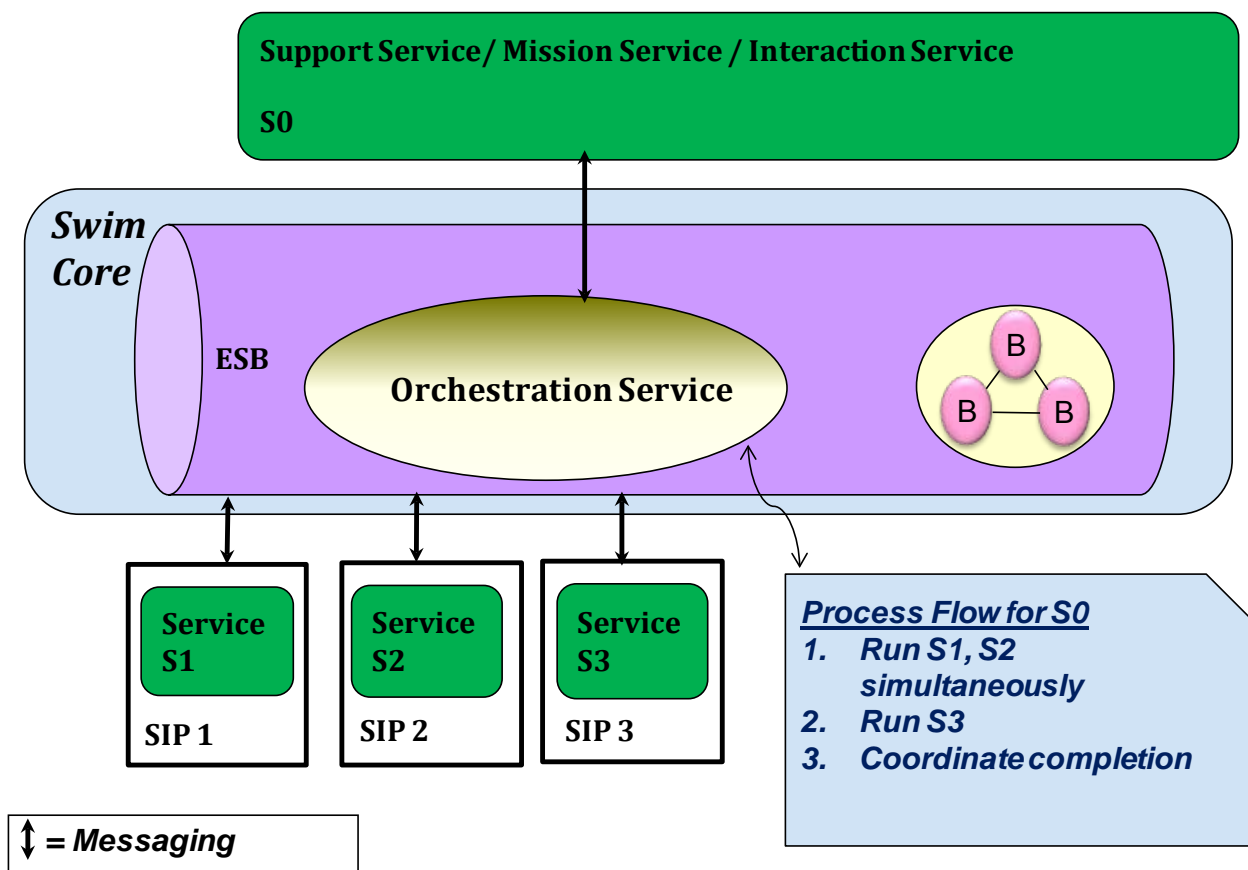
Figure 5-10. Service Orchestration in an ESB product

In Figure 5-10 above, consider a notional Mission Service or Support Service S0 that supports management of the surface traffic at airports. This service can be notionally provided in the following way: Mission Service S1 (an existing service built by SIP 1) could be a service which provides aircraft surface position data. S2 (built by SIP 2) could be a service which provides another flight ETAs (Estimated time of arrival), and S3 (built by SIP 3) could be a service which provides STAs (Scheduled Time of Arrival). An Orchestration engine can provide the co-ordination that is required between processing asynchronous requests and responses from the three services (S1, S2 and S3) since the responses can arrive in any order over an extended

5-17

period of time. An orchestration service can manage multiple interactions by correlating the requests with the appropriate responses. The input of the flight operator preferences in the processing of the results from the three services may be used to create a collaborative departure schedule from the S0 service. Different scenario results can be compiled from the processing by changing the flight operator preferences.

Interactions within a stateful business process have been abstracted to portable descriptions in the standard WS-BPEL (Web Services Business Process Execution Language). The Orchestration engine shown in Figure 5-10 is a BPEL (Business Process Execution Language) enabled engine that is pluggable in ESBs (e.g., a FUSE ESB can deploy any JBI compliant BPEL engine such as *Apache ODE*). Default databases are included in the BPEL engine to support persistent storage of state information. BPEL service engines also support databases other than their default database. The Orchestration engine can work in conjunction with an XML persistence source or a database to keep track of the process state between state transitions. Table 5-2 lists components for advanced ESB use including orchestration.

Table 5-2. Components for Advanced ESB Use

Service Functions	Service Orchestration	Service Composition
Components	BPEL Enabled engine pluggable in ESB product. Default databases included in the BPEL engine. BPEL service engines also support other external databases. e.g., FUSE ESB can plug any JBI compliant BPEL engine such as Apache ODE.	ESB product requires no special components. Optionally persistence components like databases may be used to enable additional functionality for composition.

5.1.3.9   Enterprise Messaging Security

Messaging security as it applies to Message Brokers and Web Services (implemented in WSFs, ESBs, and Web based components) are described below.

5.1.3.9.1   Message Security in Message Brokers

Securing JMS API is an integral part of securing messaging because of the JMS compliant enterprise message brokers that may form the messaging bus in the SWIM Core. Message broker is supported in a wide array of vendor products and the security controls are left to the JMS message broker vendors, since the JMS specification does not address the security requirements.

The features which will provide authentication, access control, and transport security in the JMS provider and JMS destination of the SWIM message broker are:

Authentication: A commonly used technique is that the JMS client authenticates to the JMS provider and the JMS destination in the message broker by using a username/password combination or by using digital certificates. More advanced schemes are where the JMS provider uses a Lightweight Directory Access Protocol (LDAP) directory or a repository for storing digital certificates or for storing privileged users.

5-18

Access control on JMS destinations (queues and topics): MOM products provide security through Access Control Lists (ACLs). ACLs define which end systems are allowed to send and receive messages to and from which queues and topics. JMS providers grant or deny permission to send or receive messages based on these ACLs.

JMS transport Security: JMS Specification does not address the choice of protocol to secure JMS. To secure JMS transport, most providers secure transport by the integrity and confidentiality mechanism of SSL (Secure-Socket Layer) or TLS (Transport Level Security) protocols. SSL/TLS is applied on top of the TCP/IP stack, and provides data encryption, message integrity, server and optional client authentication securing communication. For data encryption, SSL uses both public-key and private-key cryptography. SSL uses private-key cryptography to bulk-encrypt the data exchanged between two applications. The JMS provider is configured to secure transport on SSL or TLS and is applied to the JMS connection when created.

5.1.3.9.2   Java Platform API Based Security Mechanisms

If the SOA platform (e.g., message brokers, clients and applications) in the SWIM Core is using JAVA based solutions, then a JAVA based extensible security API may be feasible to use for the SWIM message brokers. Security controls like digital signing, encryption and decryption services, checking, verifying and validating authenticity of certificate chains, securing communication by applying SSL/TLS, authentication and authorization, and Kerberos based authentication can be applied. The application of these security features can facilitate single sign on between applications by using *Java Cryptography Architecture (JCA)*, *J*ava Cryptographic Extension (JCE), *J*ava Certification Path API *(CertPath),* Java Secure Socket Extension (JSSE), Java Authentication and Authorization Service (JAAS), and Java Generic Secure Services (JGSS) (in releases J2SE 1.4 and later). *Simple Authentication and Security Layer (SASL)* is a higher level authentication mechanism-neutral framework and frees up the application from being hard-wired to a specific authentication scheme (in release J2SE 5.0).

In securing messaging between the SIP client and the SWIM Core Brokers, the lowest level of security is to apply access controls in the form of ACLs on the queues and topics. If the messaging between the SWIM brokers and the SIP client does not cross any NAS boundary systems and message integrity and confidentiality is not an issue, then it may be sufficient only to enforce access controls on JMS destinations. For more stringent secure messaging, transport level security SSL can be applied on JMS, additionally messages can be digitally signed. The SWIM Broker may use a JAAS plug-in to send SIPs client credentials for authentication. The SIP client transparently connects to the SWIM Broker passing username and password and the broker in turn using the JAAS callback handler, passes the login credentials to the authentication service which returns the results back to the broker. If authentication succeeds, the broker grants connection to the SIP client, otherwise client connection fails. If further authorization is needed, an access control file is used to determine if the SIP client can access the JMS destination of the SWIM broker, or consume a message from a destination etc.

5-19

5.1.3.9.3   Securing Web Services Messaging

Most SOA deployments depend on transport level security such as SSL/TLS for authentication, confidentiality and message integrity.

WS-Security standard in addition to the transport level security provides additional means of securing SOAP messages. By using existing standards like *XML-Encryption*, *XML-Signature* and headers defined in *WS-Security*, it protects messages by digital signature and encryption-decryption specifications. To allow passing of authentication tokens between service interactions in a standard way, it uses mechanisms including username-password tokens, binary security tokens (like X.509 certificate and Kerberos ticket) and XML-based security tokens (like SAML assertion –*Security Assertion Markup Language*). WS-Security allows for encrypting the whole message or parts of the message. Messages can be also time stamped. WS-Security specification works with all SOAP versions since SOAP 1.1 WS-SecureConversation standard can secure exchanges of a consumer of a NAS services which is over multiples messages. WS-Addressing provides an XML framework for identifying web services endpoints and for securing end-to-end identification in messages.

Public key infrastructure (PKI) is essential to messaging security, for issuing, retrieving, and registering public keys. XKMS (XML Key Management Specification) defines one of the protocols for distributing and registering public keys and works in conjunction with XML Encryption and XML Signature. The PKI solution can be deployed within the NAS or by a trusted third-party. Use of WS-Trust standard of SOAP based mechanisms can help broker trust relationships between NAS systems which are using WS-Security with different security tokens.

A summary of the messaging components and messaging security (software, standards, and systems) is shown in Table 5-3.

Table 5-3. Messaging Security

Messaging Components	Messaging Security Infrastructure (Software and Systems)
Message Brokers	PKI for SSL/TLS. Possibly Java standard based security APIs (e.g., JAAS) or LDAP
Web Services Framework, Enterprise Service Bus, Components using SOAP messaging	PKI used by WS-Security, SSL/TLS. WS-Addressing, WS-SecureConversation

5.1.4   Options

Table 5-4 shows a summary of options. As shown in the table, Option 1 (EMB-01) consists of deploying a SWIM Core that consists of a basic messaging backbone built using Message Brokers. Option 2 (EMB-02) builds on this by adding platforms (hardware and operating systems) on which applications are built and hosted in the SWIM Core. Option 2 (EMB-02) is further sub-divided based on evolving service construction and service level integrations and the components used for building and deploying those services. Option 2a (EMB-2a) uses Web Service Frameworks to implement Support Services in the SWIM Core. Option 2b (EMB-02b)

further advances service level integrations and adds to those platforms by installing an ESB product suite that increases the standardization and integration of Support Services in the SWIM Core. Option 2c (EMB-02c) considers use of advanced ESB capabilities such as Orchestration to create new Support Services from existing services.

Table 5-4. Summary of Enterprise Messaging Bus Options

Option		Description	Pros/Cons
EMB-O1: Basic message brokers		The SWIM Core provides only basic messaging functions by deploying a suite of MOM products.	Pros • Low cost and risk Cons • No service construction capability in the SWIM Core • Too limited to meet the goals of SWIM, should only be considered as an interim step
EMB-O2: Service Hosting	EMB-O2a: Basic service hosting capability	In addition to the capabilities of the previous option, support for WS-* type messaging and the ability to construct Support Services is added to the SWIM core through the deployment of Web Services Frameworks and Mediation Platforms.	Pros • Allows Support Services to be hosted by the SWIM Core • Allows greater flexibility in design of each Support Service to meet specific application needs Cons • No uniform business integration environment for Support Services – may result in inconsistent designs, increasing difficulty of deployment and support
	EMB-02b: Uniform distributed integration capabilities.	In addition to the above capabilities, SWIM Core provides a uniform distributed services integration environment (e.g., Java Business Integration) through deployment of ESB product suites.	Pros • More uniform Support Service integration model Cons • ESB standardization still evolving
	EMB-02c: Advanced ESB use	ESB product capabilities (e.g., orchestration and composition) are used to create new Support Services.	Pros • Mission Services development capability added Cons • Reliability and Security not addressed in complex long running service interactions • ESB standardization still evolving

Table 5-4 provides additional summary information for each of the options in this area. All Options support a messaging backbone in the SWIM Core. The functionality of the messaging backbone expands from a JMS based SWIM Core message brokers in Option 1, to enhanced messaging of SOAP over HTTP and REST architecture, and service construction in Option 2a, by using additional components such as WSFs and mediation platforms.

Option 2b mitigates the risk of inconsistent development of service integration in Option 2a by standardizing SWIM Core architecture to an ESB product. Option 2b provides in the SWIM Core use of an ESB product with a distributed messaging core, allowing a wide array of mediation support, service construction capability, with a standardized JBI component based service and binding integration, and a standardized deployment model. SWIM Core with Option 2b capability will result in an operational environment requiring expertise in a specific class of ESB product which should reduce the long term cost of ownership.

Option 2c is the matured and advanced use of an ESB product resulting from a highly developed service infrastructure in the SWIM Core where functionally rich mission services are developed using the underlying NAS functionality consumed as services.

Security controls for messaging and web services using a security infrastructure of authentication, access control, and transport security are detailed in Section 5.1.3.9 and summarized as Security in Table 5-5.

Table 5-5. Enterprise Messaging Bus Options

	Option - 1	Option – 2a	Option - 2b	Option – 2c
Options	Messaging service provided by MOM based product	Messaging and service construction provided by MOM based products, Web Services Deployment and Mediation Platforms	Messaging and service construction provided with uniform distributed integration capabilities using ESB product	Messaging and advanced service construction provided with advanced use of ESB products
Components	Message Brokers (e.g., *FUSE ActiveMQ*, MQSeries)	Message Brokers (e.g., *FUSE ActiveMQ*, MQSeries) Web Services Framework - WSFs (e.g., *Apache CXF, FUSE Services)* Mediation based products (e.g., FUSE Mediation Router or Camel, XSLT engines, XPATH processor)	ESB e.g., some examples (not a complete list) Apache ServiceMix, FUSE ESB, IBM Websphere ESB, Sonic ESB, TIBCO Business Works, CapeClear, iWay Software, BEA Weblogic/Aqualogic, JBoss ESB, Sun Microsystems Open-ESB, CodeHaus Mule Message Brokers	ESB products with BPEL engine. Apache ServiceMix with BPEL Apache Ode. Possible use of external databases Message Brokers
Security	PKI for SSL/TLS and WS-Security. Possibly Java standard based security APIs (e.g., JAAS) for JAVA platform, LDAP, WS-Addressing, WS-SecureConversation, WS-Trust (Common infrastructure for all Options)			

5-22

	Option - 1	Option – 2a	Option - 2b	Option – 2c
Possible Deployment	Distributed Clusters of Message Brokers	Distributed Clusters of Message Brokers, Web Services Frameworks deployed standalone, or embedded in service containers. Mediation platforms deployed in service containers	Distributed Clusters of ESBs and Message Brokers	Distributed Clusters of ESBs and Message Brokers

5.2   Web Hosting

5.2.1   Scope

This section includes web application hosting platforms that can be used to support the operation of NAS Interaction Services. This includes support for both Interaction Services used by operators internal to the NAS, as well as externally visible Interaction Services made available to the public and to NAS partners.

5.2.2   Drivers

The analysis of the NAS mid-term operational concepts performed by MITRE/CAASD and documented in (Prabhu and Thomson March 2009) identified the need for user interaction services to support the NextGen concept of operations in the mid-term. Therefore there is a need to facilitate the development, deployment, and operation of these services in an efficient, timely, and secure manner in the NAS. This need is the driver for having an option for web hosting services included in the SWIM Core.

5.2.3   Analysis

The architectural components that provide web hosting capabilities are shown in Figure 5-11, in the form of a notional example of Interaction Services provided to meet the requirements of the NextGen "On-Demand NAS Information" concept. The key architectural components are Web Server platforms located within the SWIM Core for internal NAS use, as well as within the NAS Boundary Protection System, providing additional security controls for Interaction Services being made available to external (non-NAS) users. Security controls for Interaction Services are discussed in some detail in Section 5.6.3.2 .
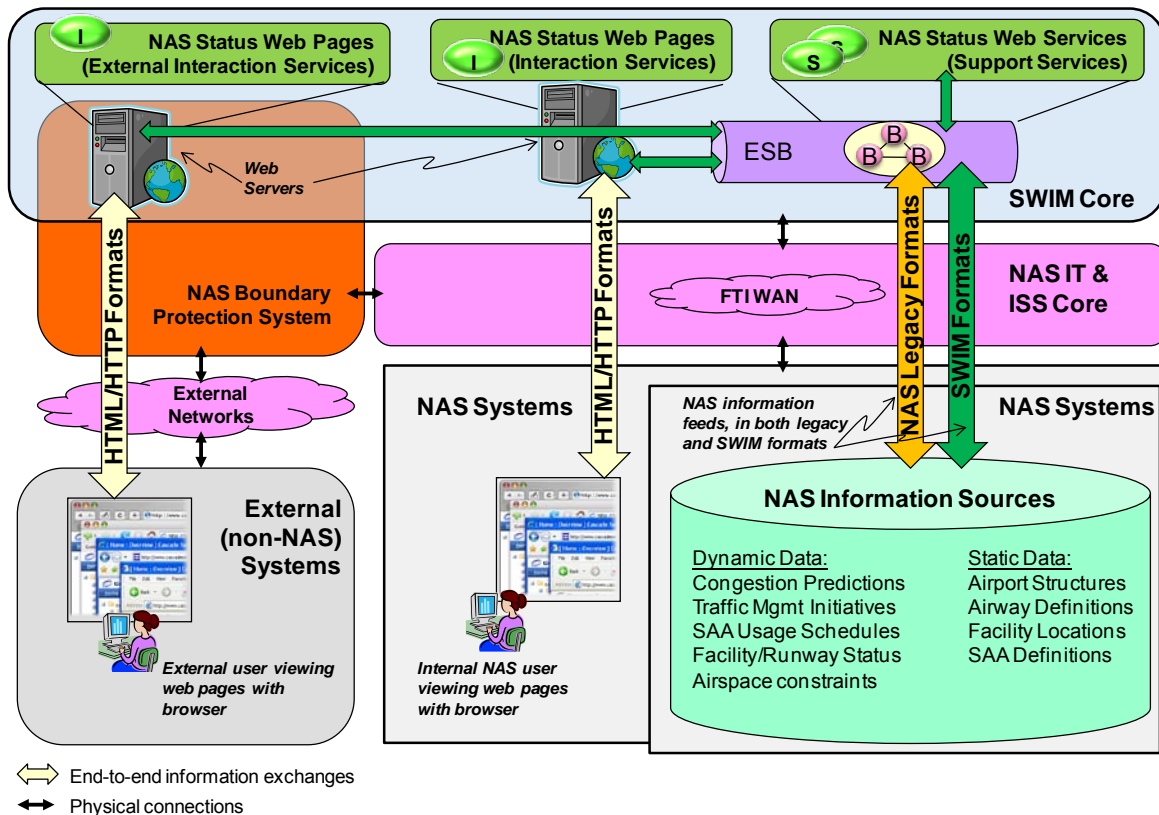
Figure 5-11. Web Hosting Capabilities – Example for On Demand NAS Information

To provide the Web Hosting Services function, the SWIM Segment 2 architecture includes web server platforms. These consist of hardware and underlying operating system capabilities (which may be considered part of the Technical Infrastructure layer of the NAS SV-4 shown in Figure 3-1), as well as a web server software platform capable of hosting web applications that provide the Interaction Services. Figure 5-11 illustrates NAS Status web pages hosted on web servers in the boundary, as well as within the interior of the NAS. The NAS Status web pages are built by accessing data from NAS Status web services. The NAS Status web services in turn access information made available by NAS Mission Services or legacy information feeds.

The components shown in Figure 5-11 are notional, and not intended to represent a specific design. Also, depending on specific application needs, additional components may be needed beyond what is shown in the figure. For example, additional components may be needed to support failover for high availability. Load balancing front-end devices may be also needed to provide the necessary performance. Design details such as these are beyond the scope of this document.

5.2.4 Options

Two options for SWIM Segment 2 are summarized in Table 5-6.

Table 5-6. Web Hosting Options

Option	Description	Pros/Cons
WS-O1: No web hosting capability	If Interaction Services are needed in the NAS in the Segment 2 time frame, they are implemented independently by SIPs.	Pros • Allows each SIP to create and operate a solution which meets their unique requirement, without any coupling or interdependency with other programs Cons • Duplicates design and implementation efforts across programs, increasing total cost • Multiple solutions in the field will increase operations costs and may require operations personnel to be trained in administering and maintaining multiple different technologies or vendor products (This could be mitigated by common product selection efforts, but solutions will still be independently operated) • More difficult to ensure security of multiple different design
WS-O2: Web hosting capability	Web Hosting Services are included in SWIM Segment 2, and utilized by SIPs developing Interaction Services.	Pros • A common solution is simpler and cheaper to operate • Security expertise can be focused on the common solution Cons • Creates dependencies across programs during the acquisition phase. A business model must be worked out in which SIPs and the hosting provider can agree on requirements (e.g., perform integration and acceptance testing) • The concept for operational support becomes more complex

5.3 Collaboration

5.3.1 Scope

This section describes architecture components to support the collaboration functions listed in Section 3.3.4.

5.3.2 Drivers

The need for SWIM to support collaboration functions is based on the NGIP analysis (Prabhu and Thomson March 2009). This analysis determined that collaboration functions may be

needed to support some of the operational concepts contemplated in the NextGen mid-term concept of operations. This analysis identified several notional use cases for collaboration functions:

- In implementing the flexible airspace management capability, en-route controllers and the traffic managers could collaborate by instant messaging, chat, and/or desktop application sharing and make re-sectorization decisions.

- In Surface Traffic Management, where decisions are to be made to mitigate ramp and gate congestion, collaboration between dispatchers, controllers and managers may result in effective co-ordination.

- In responding to information system security and other types of security incidents, efficient collection of information and coordination of response actions can be facilitated by real-time collaboration sessions.

5.3.3 Analysis

Figure 5-12 shows tools and capabilities that are available to provide collaboration function. These include:

- **Instant Messaging:**

  These are tools that provide point to point, non-persistent messaging between human users at multiple locations. Messages may be in the form of text, audio or video.

- **White Board with Annotations:**

  These tools provide a whiteboard like experience where human users at multiple locations can make marks, highlights, or notes on a blank whiteboard and/or annotate pictures, diagrams, or documents in real-time, with all participants viewing the results.

- **Screen Sharing:**

  Screen sharing tools allow the presenter to share their desktop, or the graphical user interface of a particular application being displayed on their desktop, with users at other locations. These tools may also allow a remote user to take control of the mouse and keyboard to operate the application being displayed on the presenter's screen.

- **Web Conferencing:**

  These tools incorporate much of the functionality of the above tools, allowing a user to join a conference in with an online audience and collaborate by voice, presenting and viewing presentations. The distinction between these tools and those mentioned above is that Web Conferencing tools run entirely within a standard web browser application, rather than requiring separate software applications to be installed on the users' machines.

The suite of collaboration functionality (e.g., instant messaging, web conferencing, remote desktop sharing) can be a set of different tools from different vendors. Products mentioned here do not represent a complete list but illustrates the variety of options available. Some enterprise

messaging tool products are *IBM Lotus Instant Messaging & Web Conferencing*, *Sun ONE Instant Messaging*, *Sigaba Secure IM*, *Effusia Business Messenger*, *WiredRed e/pop*, *Ipswitch Instant Messaging,* etc. The *Adobe Connect Now* product creates free meetings online to have video calls, whiteboard and share files. *GoToMeeting* Conferencing Now software allows screen sharing with many features. *VoIP Communicator* software allows free online conversations between PCs.
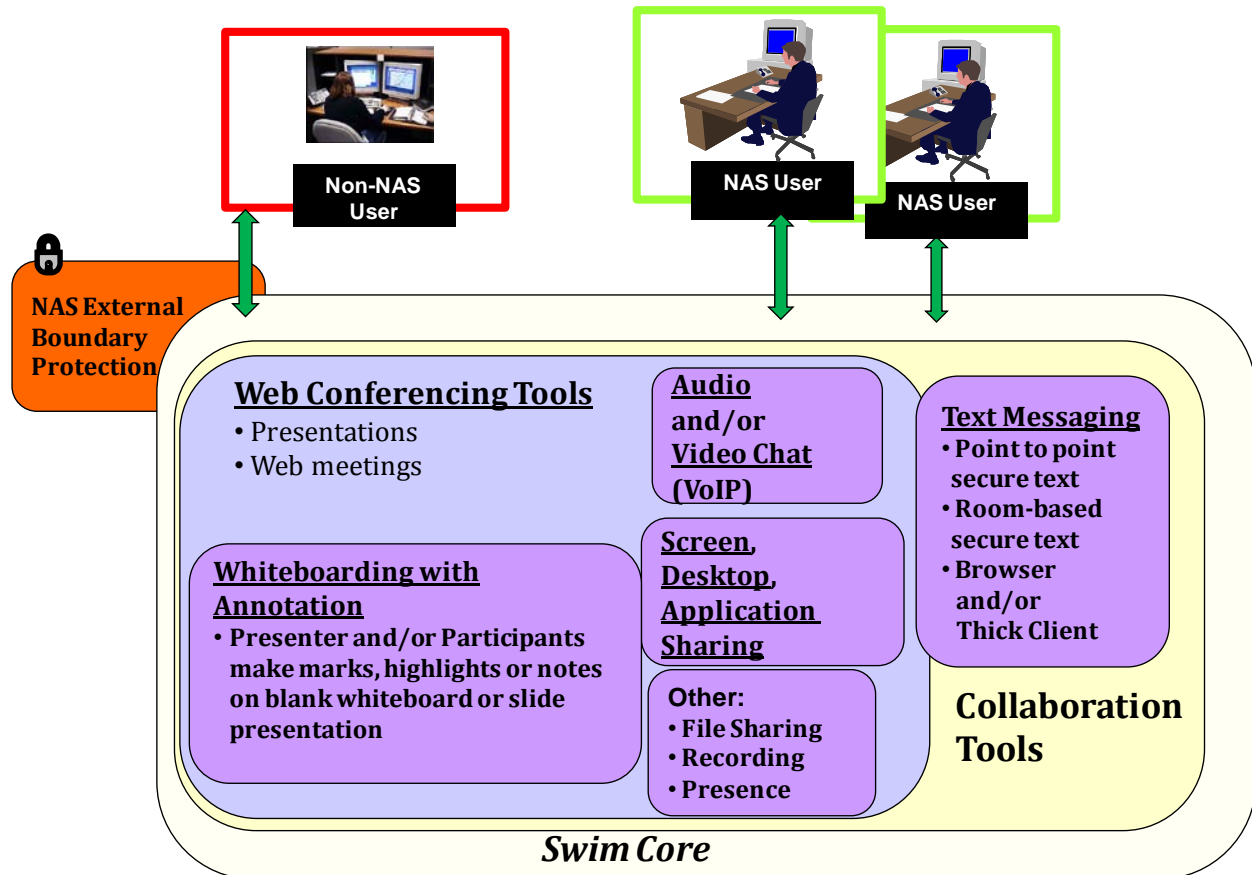
Figure 5-12. Collaboration Capabilities in SWIM Core

Use of these tools in the NAS will require security mechanisms to provide functions such as identification and authentication, authorization, and confidentiality. For collaboration with non-NAS users, boundary security controls will be needed to allow the necessary connectivity and data flows between NAS and non-NAS systems.

Administration of these tools is required to provision for user access. Logging and archival of activity on tools, anti-virus on products with instant messaging exchange and file sharing capabilities, are some of the needed administrative functions that will be needed to support collaborations tools.

5.3.4   Options

Two options for SWIM Segment 2 are summarized in Table 5-7.

Table 5-7. Collaboration Options

Option	Description	Pros/Cons
C-O1: No Collaboration Tool Support	Collaboration tools are not supported.	Pros • Allows each SIP to create and operate a solution which meets their unique requirement, without any coupling or interdependency with other programs • Existing voice based collaboration in NAS may be sufficient • If needed, collaboration tools can be deployed onto administrative (non-NAS) systems Cons • If collaboration is implemented by SIPs, this duplicates design and implementation efforts across programs, increasing total cost
C-O2: Collaboration Tool Support	Wide ranging collaboration tools are supported.	Pros • Facilitates improved operational efficiency in the NAS by providing operators with flexible tools • A common solution may be cheaper to implement and operate than individually developed tools • Security expertise can be focused on the common solution, resulting in a less overall risk Cons • Introduces new protocols and data flows, creating potential security risks • Integration of collaboration tools with existing NAS display systems • Cost to acquire, deploy, and support these tools

5.4   Interface Management (Registry)

5.4.1   Scope

While Interface Management can be broadly defined to include governance activities intended to promote interoperability between service providers and consumers, in this document we discuss only service information publication and discovery. This should be consistent with the SWIM Segment 2 Core Services Enterprise Architecture Views document and Section 3.4.5 in this document.

This section focuses on how service discovery will take place in the SWIM Segment 2 timeframe along with how it fits within the overall Segment 2 architecture. Both design time and run time operations will be addressed. Data architecture is not discussed in this document.

Note that in general a registry and repository have distinct definitions. A Service Registry contains information about services, such as the service definitions, interfaces, operations and parameters while a Service Repository (also Metadata Repository) contains additional metadata, such as service policies, and contracts. Repositories also contain service metadata such as version, status, relationships, and information that governs the service usage (Interface Requirements Document, SWIM/User, NAS-IR-43070001 October 2008). However, in this document we mostly use the term "registry" to describe a complete set of registry and repository functions except for discussions where functions that are specific to a repository such as policy management are described.

5.4.2   Drivers

There are several drivers that establish the need for a mechanism for discovering services as well as store and manage metadata in support of SOA governance activities. The drivers include:

SWIM Segment 1 architecture and subsequent efforts have established the importance of a Service Registry if an organization were to create a SOA based environment.

Service Registries have been key enablers of SOA in organizations that have successfully implemented SOA.

The SWIM Registry Interface Requirements Document (IRD) captures interface requirements between the SWIM Registry and SWIM users.

Prototyping efforts both in MITRE/CAASD as well as the FAA.

The GEIA report that further validated the need for a SWIM provided registry (FAA SWIM Program - Segment 1 to Segment 2 Transition - Industry Input December 2008).

The SWIM Registry should support all NGIP capabilities identified in the concept of use work that was done for SWIM in the Mid-Term (Prabhu and Thomson March 2009)

5.4.3   Analysis

This section describes SWIM Segment 2 registry capabilities that allow users to discover services, as well as registry capabilities that support SWIM operations through an interface with SWIM service management capabilities. Service Location Transparency will also be discussed and its operation shown in a run-time context. Based on current understanding of the limited maturity of run-time registries, SWIM Segment 2 should continue to use a design-time service registry with appropriate interfaces needed to support SWIM Operations.

5.4.3.1   SWIM Registry

SWIM Segment 2 will continue to have a central design-time registry as in Segment 1. The existence of such a registry does not preclude SIPs from having their own registries for use in their domains while synchronizing information on relevant services with the central registry. As registry protocols and technology mature the level of automation for synchronization with the SWIM registry could increase.

The SWIM Service Registry consists of two distinct but synchronized pieces discussed in Section 5.4.1. It must provide sufficient availability to meet requirements that will derive from its intended use, and meet NAS and SWIM Information System Security requirements.

To support discovery of service information by users who may not be connected to the NAS operational network (e.g., developers, system engineers), the registry will be accessible via the FTI Mission Support network. However, in Segment 2, an interface with the registry from the NAS operational network will be needed to support SWIM operations. To provide this connectivity while conforming to the NAS Security Architecture, the registry will access the NAS environment via a gateway within the External Boundary Protection (EBP) System discussed in Section 5.6.

As shown in Figure 5-13 the registry concept represents a "staging" and "production" registry, similar to the plan adopted for Segment 1, in order to facilitate a human-in-the-loop certification process. Note that this is a notional depiction and specifics could change subject to Segment 2 governance guidelines. For instance "staging" here could also mean forms waiting for Governance approval and not necessarily an actual registry being used in an automated fashion. Registry interfaces with publishers, consumers, administrators and Segment 2 SWIM Operations elements are discussed below.

5.4.3.1.1 Publishing by a Service Provider

The registry will support the publication of service information by service providers subject to the governance guidelines for Segment 2 and as stipulated in the SWIM Registry IRD.
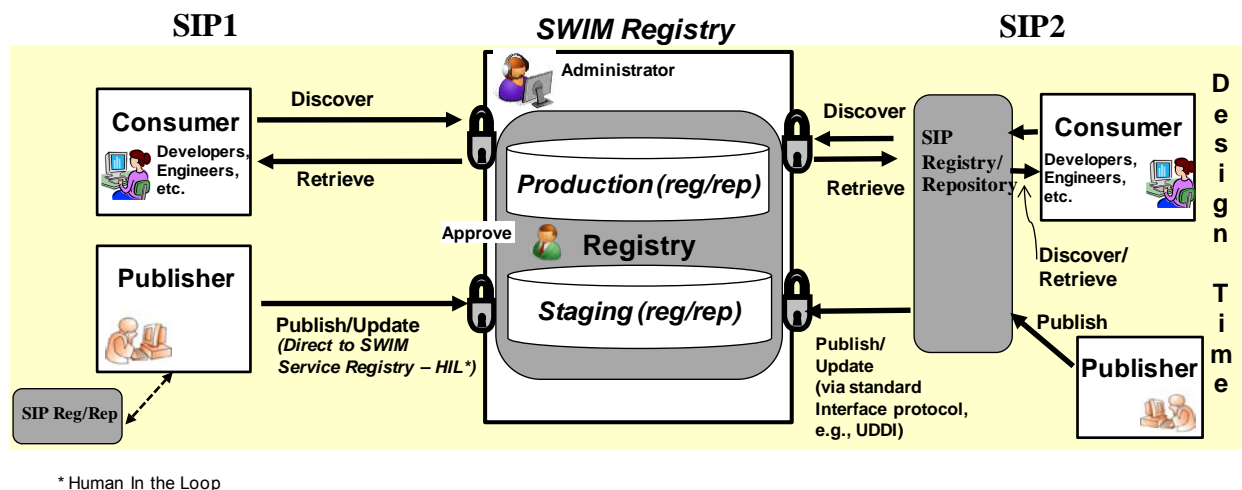
Figure 5-13. SWIM Service Registry Support for User Discovery of Services

Figure 5-13 shows two possible ways service providers (SIPs) can interface with the staging piece of the SWIM registry. Both methods involve the approval of a SWIM certification authority before contents get published to the production piece of the SWIM Service Registry. In the first method, a user (publisher) directly accesses the SWIM Registry, subject to access control. The publisher submits service information to the staging registry via a user interface

(e.g., web browser) at which point the person in charge of certifying registry content reviews the information and accepts or rejects it per governance guidelines. If accepted it would be moved from the staging registry to the production registry at which point consumers can discover it. In the second method, service information is submitted via a SIP-specific registry (e.g., UDDI based SIP registry). Again the submitted content would have to be reviewed and certified before deployment to the production registry.

5.4.3.1.2   Service Discovery by a Consumer

The registry will support the discovery of service information by service consumers subject to governance guidelines for Segment 2 and as stipulated in the SWIM Registry IRD. Service consumers must first register to qualify as users of the registry before discovering and retrieving service information. Appropriate security controls will be in place to prevent unauthorized access to service information and the registry itself. There are two possible ways consumers could discover information on the production SWIM Service Registry. One is by directly accessing the SWIM Registry after the initial registration and approval process. The second method is by using other registries (e.g., a SIP registry) to discover the SWIM service registry. For example, some other FAA service registries, which are currently in the design stage, will reference the SWIM service registry as an affiliated registry as discussed in the SWIM Registry IRD for Users (Interface Requirements Document, SWIM/User, NAS-IR-43070001 October 2008).

5.4.3.1.3   Registry Security

The SWIM Service registry will comply with FAA security processes and requirements in general. User identification, authentication and authorization need to also be supported. The Security section in this document will address SWIM as well as NAS security measures that will apply to all SWIM systems.

5.4.3.1.4   Registry Administration

The SWIM Registry will have an Administrative entity (person or group) which will be responsible for service registry functions and registry operations. This activity will be considered part of Swim Operations discussed in Section 5.5.

5.4.3.1.5   High Availability

The SWIM Registry needs to have sufficient availability to not only support design-time activities but also production and governance related work. Providing the necessary availability could entail a minimum of two groups of two registries in different locations in hot stand-by mode with database replication.

5.4.3.1.6   Policy, SLA, and Management Data Exchange

While the SWIM Registry in Segment 2 will continue to be a design time entity as in the first SWIM Segment, it will have an important relationship with a key run-time element of SWIM. This element is the SWIM ESM which will include such functions as SLA compliance checks and policy enforcement in addition to service fault and performance monitoring. It is an integral

part of the overall SWIM Operations activity which will include system and network management as well as other traditional operations center functions such as help desk. The relationship between the SWIM Registry and ESM as depicted in Figure 5-14 is discussed below.
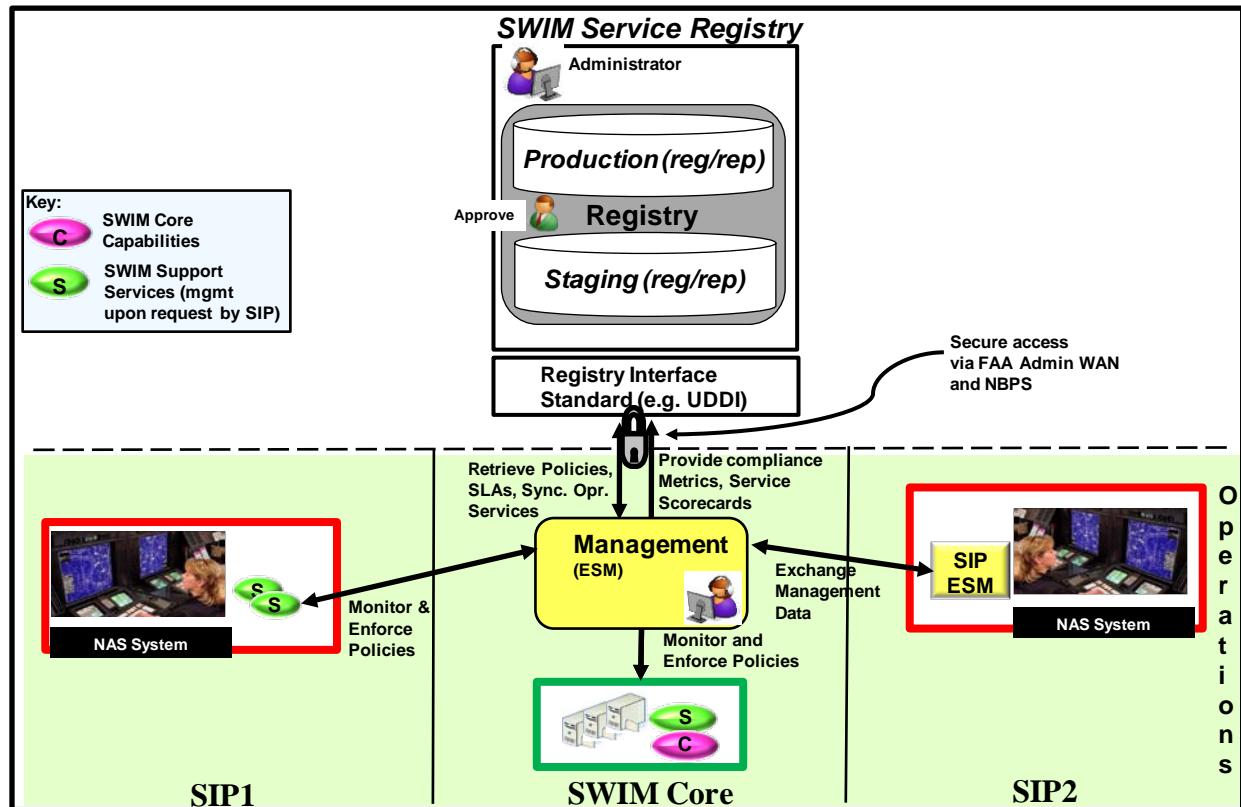
Figure 5-14. SWIM Service Registry Interface with the ESM Capability of SWIM Operations

SWIM Operations configures and runs the ESM to discover SWIM operational services (core services, support services, and mission services) both in the SWIM Core as well as in SIP environments where there is an agreement for SWIM to directly monitor services. The discovered list of services is checked against the active or operational services list in the SWIM Registry at initial discovery time and as needed thereafter for governance compliance purposes.

On the governance side the SWIM Registry provides approved policies and service contracts (SLAs) to the ESM from its repository piece as per SWIM Governance. The ESM enforces policies as well as checks for SLA compliance and submits metrics and service scorecards back to the registry. An example of an interface that could support some level of interaction and data exchange between the Registry and ESM is a secure Universal Description, Discovery, and Integration (UDDI) interface. Other capabilities are to be used subject to maturity of run-time SOA Governance capability during the Segment 2 timeframe.

5.4.3.1.7   Registry's Role in Service Lifecycle

The SWIM Registry will support service change and version management [3] as well as service dependency tracking as part of its service lifecycle support role. Because of the specific SWIM and NAS environment this role is totally dependent on the governance process for service lifecycle management and information fed by SIPs regarding their services. Figure 5-15 adapted from (Wilkes April 2005) shows how the SWIM Registry can be positioned relative to service providers and consumers as well as other players like service management. The registry's important role in the lifecycle of a service is also shown based on the service related interactions that take place between the service consumption and service provision bars shown in the figure.
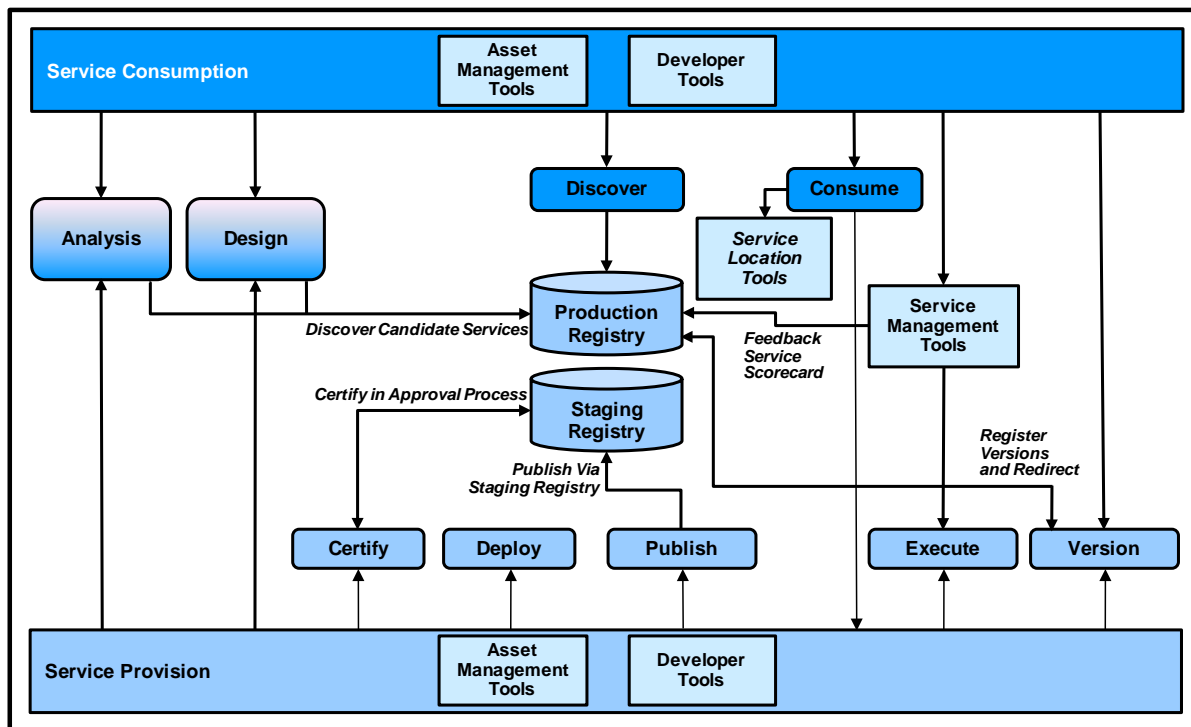
Figure 5-15. Registry Role in Service Lifecycle

5.4.3.2   Service Location Transparency

Service location transparency is a run-time function that allows consumer client applications to dynamically determine an end point instance of a desired service. This may be used in several ways, including the following:

- Simplifying administration and configuration of service consumers, by obviating the need to pre-configure them with the locations of service end points

- Load balancing, by providing dynamically selecting end points of service providers based on the current ability to handle the load

---

[3]   The notion of version management here is referring to the capability of the registry to accommodate different versions of service instances as provided by SIPs or service providers.

- Support for recovery from service failures. For example, if an instance of a given service is down, an alternate service instance endpoint is provided to the consumer client.

To achieve service location transparency, some form of Service Locator functionality is necessary. This functionality is a run-time capability which facilitates the discovery of service endpoints by client applications. In general, to achieve location transparency, consumer client applications will need to retrieve service endpoint information by sending a request to some form of Service Locator before consuming a service. Figure 5-16 depicts this Service Locator functionality in general terms.

There are different ways that this functionality could be implemented as discussed below:

- A Service Locator can be implemented as a custom-built web service in which case provider services register their endpoints with the locator at start-up and consumer client applications obtain endpoint location information of different instances of the same service (depending on which service is available) by querying the Locator. Once the endpoint location information is obtained, target web services can be consumed. An example of such a Locator is the Artix Locator from Progress Software.

- Use capabilities built into some ESB products, as mentioned in Section 5.1.3.6.

- Use a registry product in a run-time manner. However, to date, there do not appear to be extensive run-time use of registry products in this way in large operational environments.

The ability to support failover is often cited as the driving reason for having service location transparency. However, if service location transparency is to be used to support failover, then the service locator must have some way of knowing which services have failed and which are currently available. In theory, this may be done by integration with ESM tools, or by directly monitoring service availability. However, maintaining knowledge about which specific endpoints are available at any moment introduces an infrastructure burden that may be unreasonable.
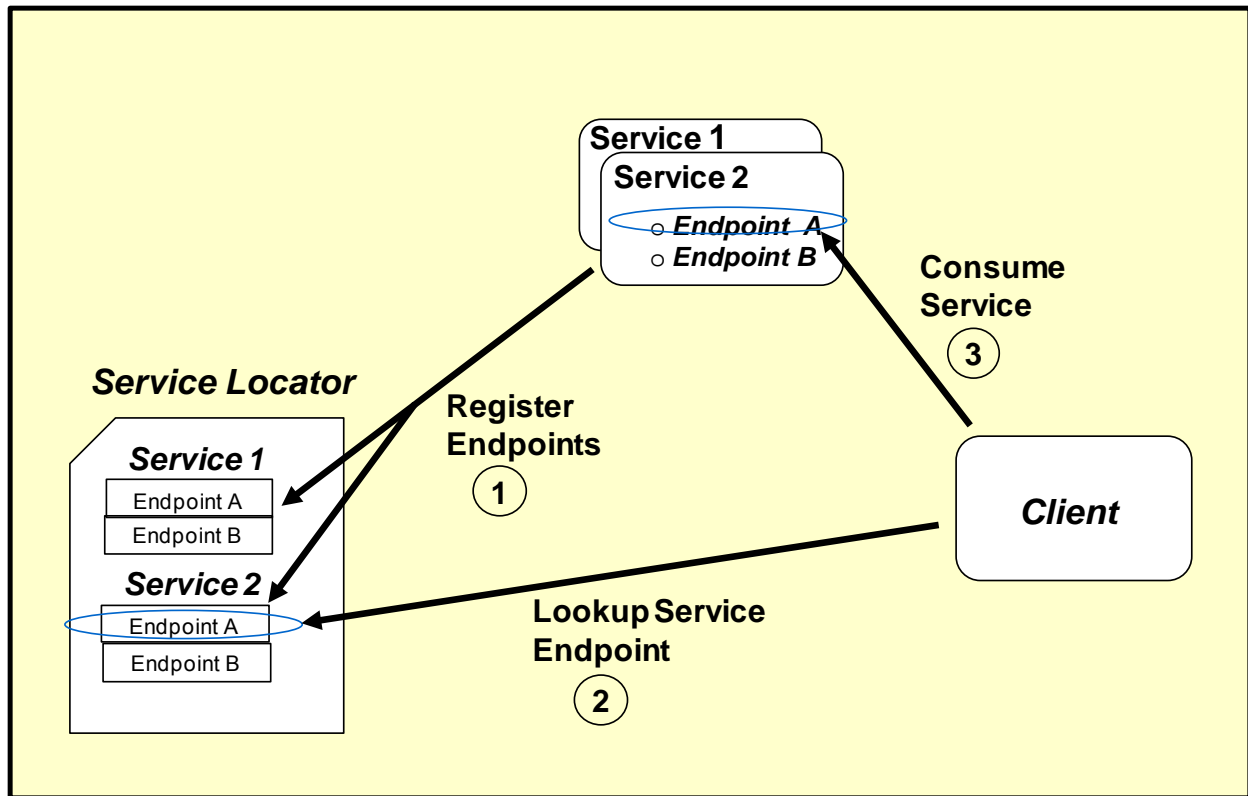
Figure 5-16. Service Endpoint Registration Based Locator

5.4.4 Components

Components for the Service Discovery SWIM Core Service are listed in Table 5-8 below. Also listed are related components that fulfill governance related registry functionality as well as service location transparency:

Table 5-8. Components for Service Discovery and Related Functions

Function	Component
Service Discovery	Design-time Registry (e.g., Systinet, Oracle, and IBM's registry products)
Policy, SLA, Security Policy Management, Service artifacts like schema, human readable documents (primarily Governance Support)	Metadata Repository (e.g., Systinet and IBM repository products, freebXML)

5.4.5 Options

There are two options identified for the SWIM Service Registry in Segment 2 as shown in Table 5-9. The first option, REG-01, calls for a registry similar to what is planned for use in the SWIM

Segment 1 timeframe. It will have limited or no capabilities (e.g., no automated interface with service management capability of SWIM Operations).

The second option, REG-02, calls for a registry with an interface with SWIM Operations (i.e., the ESM element) for retrieving policy and SLA compliance data as well as providing governance related policy information for enforcement. Below is a summary of the capabilities of the registry in REG-02:

The ability to use ESM interfaces for retrieving run-time statistics and providing governance related policy information will depend on the maturity of standards and/or products.

Information on service instances and their location is initially obtained from and occasionally synchronized with the SWIM Registry.

Service failure updates are obtained from the service management system subject to the type and sophistication of the management system.

Table 5-9. Summary of Service Discovery Options

Option	Description	Pros/Cons
REG-O1: SWIM Service Registry with limited capabilities	Only the SWIM Service Registry with a limited set of capabilities (e.g., no automated interface with ESM in SWIM Operations).	Pros • Simpler • Not dependent on standards that are not mature or limited Cons • Cumbersome to use • Prone to mistakes because of extensive "human in the loop" • Less efficient from operations perspective
REG-O2: SWIM Service Registry with advanced capabilities and a service locator for run-time use	The SWIM Service Registry will have advanced capability to support policy and SLA data exchange with ESM in SWIM Operations.	Pros • Better and effective governance • Efficient and easier to manage from operations perspective Cons • Policy and registry interface standards are not as advanced in other SOA areas like messaging • No industry consensus yet on existing registry standards

5.5   Enterprise Service Management (ESM)

5.5.1   Scope

The primary focus of the discussion in this section is ESM, which includes service fault and performance monitoring and reporting, policy enforcement, SLA compliance checking, and service scorecard generation. In addition to ESM, the overall system management context under

which ESM operates has to be explained in order to fully understand the SWIM architecture related to ESM. Operational concepts are discussed to set the stage for more in depth analysis of ESM's role in SWIM Segment 2.

The following points about ESM provide context and bound the discussion that will follow:

- ESM provides a complete view of a service environment and can perform active and passive management.
  - Active management (e.g., policy enforcement) is important for governance support.
  - Passive management (e.g., metrics collection for performance and availability) is important for service quality identification.
  - The scope of view provided by ESM is determined by the set of systems that the ESM capability is allowed to view and manage, which is decided as the outcome of a governance process.
- ESM can provide real time monitoring and reporting of fault and performance.
- ESM operates at the service level and complements traditional management systems such as system and application management tools.
- ESM is just one element of a larger IT support operation with help desk support, including troubleshooting when problems occur.

5.5.2 Drivers

There are several drivers that establish the need for a centralized ESM solution in SWIM Segment 2.

The federated nature of SWIM Segment 1 does not allow for an end-to-end view of service management data, which will make troubleshooting to resolve service failures across SWIM more difficult. An opportunity to address this shortcoming arises in SWIM Segment 2 by including ESM within a larger SWIM Operations capability that would include system, application, and network management services. This will enhance the ability to address problems before they occur and increase the reliability of the SWIM Core and SIP services.

Prototyping efforts within MITRE/CAASD clearly indicate the need for such management capability as well as the availability of sufficiently mature ESM tools to provide this capability. It is common industry practice to have mechanisms for managing and troubleshooting service problems. Furthermore, because the more advanced ESM tools have the capability to support governance functions they have been widely embraced by industry. The industry consortium report (FAA SWIM Program - Segment 1 to Segment 2 Transition - Industry Input December 2008) further validated the need for an ESM solution.

The SWIM ESM should support all NGIP capabilities identified in the document titled Concept of Use for SWIM in the Mid-Term (Prabhu and Thomson March 2009). Two of these capabilities are Flexible Airspace Management and Point in Space Metering.

5.5.3 Analysis

This section first establishes a context for ESM within SWIM Operations and how it fits in with other resources used to manage systems and applications that are part of the SWIM Core. This is followed by an ESM-specific discussion on how to evolve from the Segment 1 federated environment to one where a central ESM interacts with SIP ESMs or directly manage services outside the SWIM core based on program level agreements with interested SIPs. ESM's role in governance and its interaction with policy and SLA management systems for policy retrieval and submittal of metrics will also be addressed. Help desk support and collaborative troubleshooting to resolve service related problems will be discussed. All ESM functions listed in Section 3.3 are analyzed.

5.5.3.1 ESM and SWIM Operations

As discussed in Section 2.4, in the SWIM Segment 2 timeframe the SWIM Program office will have the responsibility to develop and deploy a "SWIM Core" containing a set of consolidated core services. Some services (Support Services) developed by a given NAS System Program could be deployed to the SWIM Core. These are managed and operated along with other resources like computing platforms by operations staff. One of the systems that this operations staff would operate is the ESM. Figure 5-17 shows the various interactions that SWIM Operations and ESM tools have with SIP service management systems. ESM tools at the SWIM Operations Center will:

- Monitor fault and performance of services and collect metrics on services running in the SWIM Core

- Receive a subset of service management data gathered by SIP ESM tools

- Make a "mosaic" of cross-SIP service management information available to all SIPs via a web portal

- Enforce policies on SWIM Core services and check for SLA compliance

- Generate service scorecards and submit them to the SWIM Registry

- Conduct help desk operations and collaborate with SIP operations staff
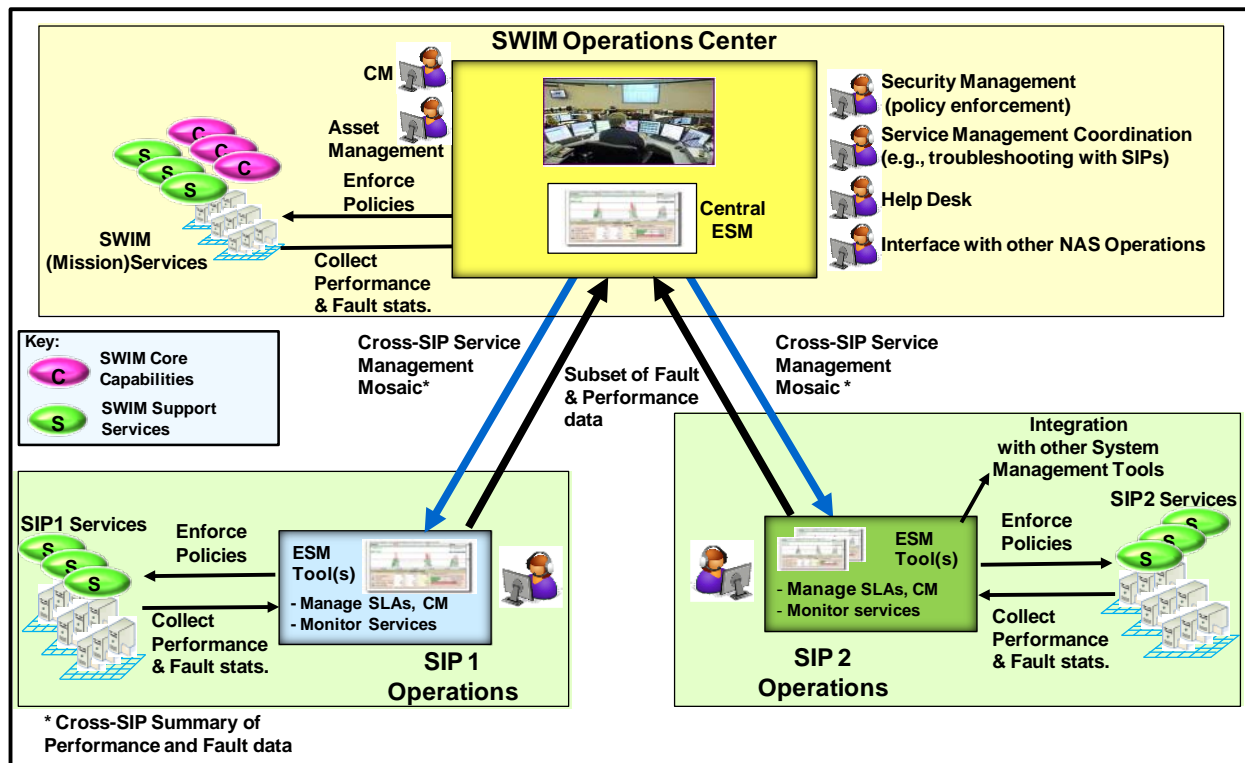
Figure 5-17. ESM and SWIM Operations Concept

ESM or a service management system at a given SIP would:

- Monitor fault and performance of services and collect metrics on services running in the SIP environment

- Provide a subset of service management data collected at the SIP level per Program Level Agreement (PLA)

- Retrieve cross-SIP ESM data from SWIM Central ESM as needed

- Collaborate with other SWIM Operations staff using tools like chat and voice for troubleshooting (see Figure 5-19)

5.5.3.2   Centralizing ESM and Interaction with SIP Domains

Moving from a federated service management model to a centralized one with most SIPs continuing to do their own system management comes with its own challenges. This hybrid model is called "shared service management" in (FAA SWIM Program - Segment 1 to Segment 2 Transition - Industry Input December 2008). In this model there should be some level of management data exchange between the central ESM capability and those in SIP domains. However, as of now and in the foreseeable future, there is no service management standard that is on track to be adopted by the ESM community. Without a standard, a management system from one vendor implemented in one domain can't exchange data with a management system from another vendor implemented in another domain. A technical solution might be for each

management system to deploy agents into each other's domain. However, this could be seen as intrusive and unacceptable by the domain stewards. One possible workaround to this problem is to consider exchanging data using XML. The central ESM (that is, the ESM in the SWIM Core) would only get a subset of the metrics collected by the SIP ESMs in their domains. The extent of this subset would be determined via a Program Level Agreement (PLA). Table 5-10 shows one possibility (notional) of the types of data that could be provided to a central ESM in SWIM Operations by a SIP ESM. For instance basic fault data (i.e., service up or down or response time could be sufficient to have an understanding of the state of a given service). Once the central ESM has similar data from a number of SIPs it can create a cross-SIP service failure status page and could possibly update that information at periodic time intervals. This will create an end-to-end view of the enterprise at a basic level. Performance data, such as service response time, could be treated in a similar manner. This capability has been identified in Section 5.5.5 as one of the options (Option 2) that can be considered in determining ESM capability for Segment 2. Alternately the central ESM capability could handle policy enforcement and SLA compliance related data in order to effectively support the SWIM governance process. This capability, also shown in Table 5-10, has been identified as Option 2c in Section 5.5.5.

Table 5-10. SIP ESM Data Provided to Central SWIM ESM in Segment 2 (Notional)

Potential SIP ESM Capability		Information Provided to Central ESM	
		Basic *	Advanced **
Fault	Service up/down	x	x
	Exceptions		
Performance	Throughput		x
	Response Time	x	x
	Availability		x
Policy	Security	x	x
	Performance		
	Logging		
SLA	SLA compliance checks mostly based on fault & performance related thresholds		x

* **This maps to Option 1 discussed in Section 5.6.5**

** **This maps to Options 2a and 2b discussed in Section 5.6.5**

Figure 5-18 depicts the management data exchange discussed above by showing three kinds of data exchange. In all three cases of SIP service management capability there is no agent

5-40

deployed from the service management system that is in SWIM Operations (central ESM). This has significance in that it shows that the central service management system does not have to be intrusive in SIP environments unless of course a SIP requests it. One connection shows an XSLT type XML transformation taking place in the central ESM. Some of the advanced ESMs have the capability to configure such facilities within the tool. The advantage of using this method to exchange basic management information is that it:

- Is non-intrusive in that Central ESM agents don't have to be deployed in SIP space

- Uses XML for exchanged data format except where the same ESM platform is used by SIPs

- Makes consolidated service management information available to all SIPs
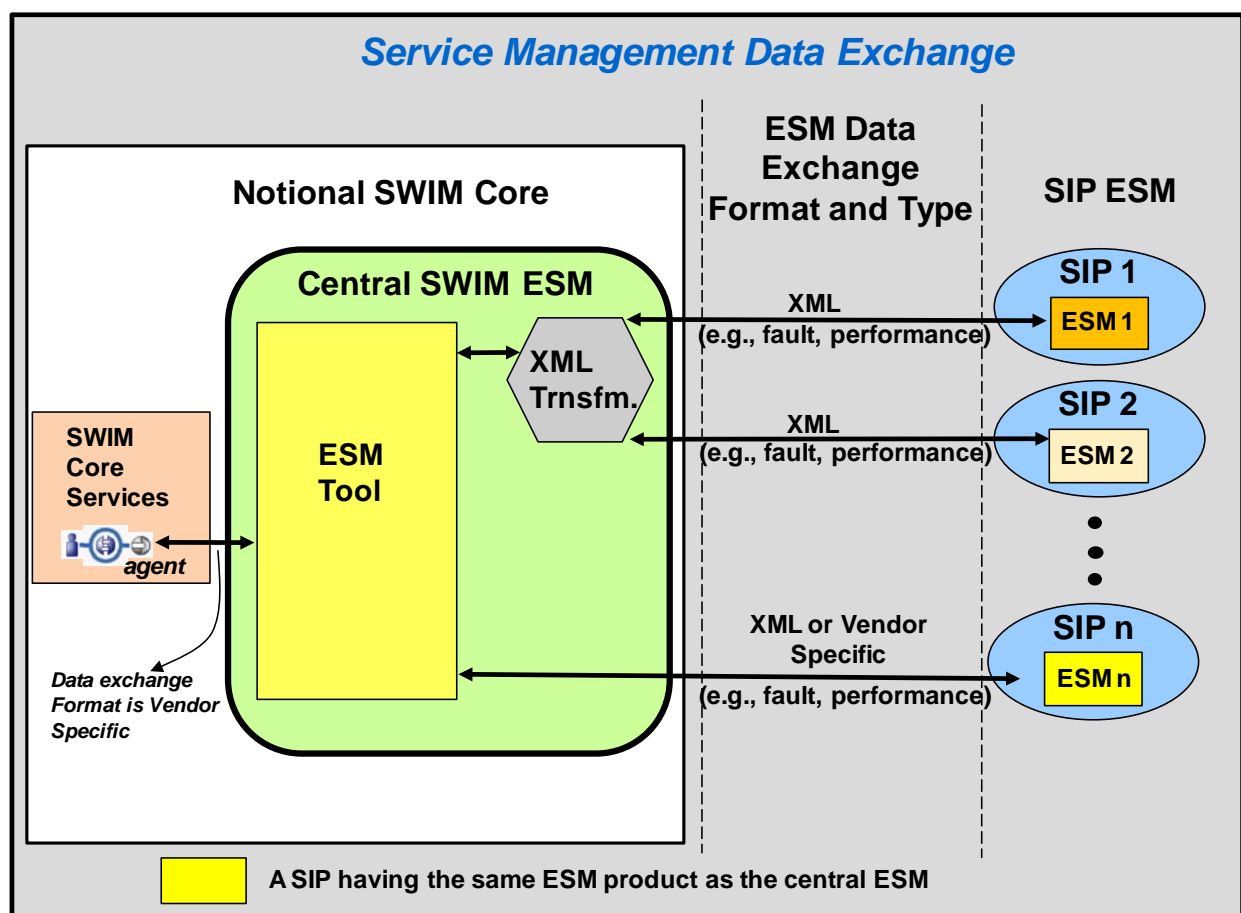
Figure 5-18. Service Management Data Exchange

Another workaround for the lack of common service management data exchange between different ESM product is the standardization of ESM products across SIPs. This falls in the realm of SWIM governance and the creation of PLAs.

5.5.3.3   Policy Enforcement and SLA Compliance Checks

An important run-time capability of an ESM tool is policy enforcement. Typical ESM solutions have policy enforcement capabilities although most current implementations tend to primarily enforce security policies since other types such as QoS have not come far along the standards track. The policies that the ESM acts on at run time are retrieved from other governance tools like the metadata registry using protocols such as UDDI.

SLAs are also checked and compliance information logged. This information is then sent to the metadata registry. ESM tools can also create service scorecards which encompass performance and SLA compliance among others. The SLA compliance related data is sent to the metadata registry for governance related assessments and service quality tagging. Service quality tagging impacts the level of usage of a service by new client applications (based on governance and developer determinations). ESM tools with SOA/Governance management capabilities are emerging and could possibly store policies and SLAs.

5.5.3.4   ESM Collaboration

The ESM Help Desk would be part of an overall Help Desk at the SWIM Operations center where problems from system failure to network malfunction to service failure are resolved through different levels of troubleshooting effort. It is the initial point of contact for assistance when users call with SWIM related issues. Part of the problem resolution entails troubleshooting and this is done in collaboration with site Tech Ops Desks and other NAS Help Desks like FTI. Figure 5-19 shows how help desks at different levels in the NAS collaborate during the problem resolution process. Collaboration is done via telephone, office automation tools, and chat. Note that what is shown in Figure 5-19 does not preclude remote administration of systems and services by SWIM Operations.

When a trouble call comes in a SWIM Ops staff assigned to the duty would initiate a trouble ticket via a trouble ticketing system like Remedy. The problem is assigned to the appropriate help desk support staff and if it is resolved right away the trouble ticket is closed and the resolution logged for future reference and help desk procedure updates. If the problem persists a sequence of troubleshooting could take place at the SIP Tech Ops as well as SWIM Tech Ops levels. The function that equates to this in Figure 3-1 is "Service Diagnostics".
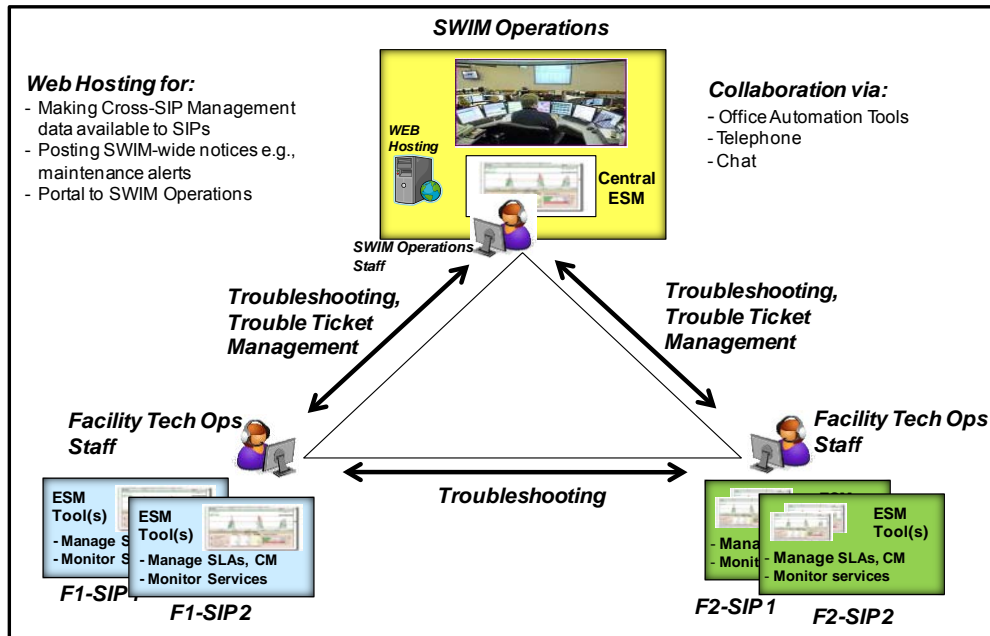
Figure 5-19. ESM Collaborative Troubleshooting and Problem Resolution

5.5.4 Components

ESM Components are listed in Table 5-11. Note that although the examples given do most or all of the functions listed, based on their requirements an organization implementing the functions could use separate products for some of the functions.

Table 5-11. ESM Components

Function	Component
Fault Monitoring and Reporting	Service Management Tool (e.g., Amberpoint, Actional)
Performance Monitoring and Reporting	Service Management Tool (e.g., Amberpoint, Actional)
Policy Enforcement and Metric Collection	Service Management Tool (e.g., Amberpoint, Actional)
SLA Compliance and Metric Collection	Service Management Tool (e.g., Amberpoint, Actional)
Service Scorecard Generation and Reporting	Service Management Tool (e.g., Amberpoint, Actional)

5.5.5 Options

The Shared Services Management model provides a good solution for managing services in SWIM Segment 2. It is very much applicable to the NAS and a viable option for implementing ESM. With this as an underlying solution for SWIM Segment 2 ESM capability, three alternatives, ESM-01, ESM-02, and ESM-03 are outlined and summarized in this section as

shown in Table 5-12. In the case of ESM-01, application and systems management capabilities in SWIM Operations manage only SWIM message brokers and associated systems. This option corresponds to option EMB-01 discussed in Section 5.1.4. Since there are no services to be managed in the SWIM Core there is no centralized service management.

Under options ESM-02 and ESM-03:

- SIPs continue to manage services in their own environments but also send a subset of their ESM data to the central ESM (PLAs should be involved)

There will be a central ESM which:

- Will have a limited end-to-end service management view based on some metrics received from SIPs

- Will also manage "support services" deployed and managed as part of the SWIM Core

- The central ESM

  - Will make a "Cross-SIP" Service Management data (including one for support services) available to all SIPs

  - Will obtain management data from SIPs in a non-intrusive fashion using XML as a basis for data exchange (no "intrusive" agent deployments in SIP space)

SWIM Operations roles will include:

- Help desk support and collaborative troubleshooting with SIP ESM operations

- Coordination with other NAS system and network management operations including the FTI Network Operations Center (NOC)

Table 5-12. Summary of Options for ESM

Option	Description	Pros/Cons
ESM-O1: SWIM Operations Management of SWIM Message Brokers	SWIM Operations manages only the message brokers, no centralized service management.	Pros • Can use traditional application and system management tools • Less complex management environment Cons • No end-to-end view of services in SWIM affiliated domains (NAS programs) • Lack of service fault and performance "mosaic" created from service management data across SWIM results in cumbersome troubleshooting and problem resolution

5-44

Option	Description	Pros/Cons
ESM-O2a: ESM with some Fault and Performance Management	Only fault and performance management for SWIM services.	Pros • Simple and more in-line with traditional application management • May be better for a small start of a central ESM in SWIM Cons • Minimal or no support for governance • Minimal impact on overall long term service quality
ESM-O2b: ESM-02 plus advanced ESM capabilities	The ESM will do more fault and performance monitoring plus other advanced functions such as policy enforcement, SLA compliance, and service scorecard generation check. Furthermore, run-time synchronization with a service locator could be supported.	Pros • Better and effective governance • Improved service quality as a result of service scorecards Cons • Policy related standards are not mature • More complexity • Some custom work may have to be done to enable updating or alerting a service locator with service "up" or "down" information

5.6   Security

5.6.1   Scope

This section describes not just the controls that will be used to secure SWIM systems and information content, but also how SWIM contributes to the overall security of the NAS.

Note that in this context the term "security" refers to ISS, sometimes referred to as "cyber security". It does not include other aspects of security, such as NAS airspace security.

There are different security controls that will need to be deployed at different locations and at different logical "levels" within the NAS. For example, there is a need for network layer security controls deployed within local and wide area networks, as well as application layer security controls deployed in end system software applications. Also, while some supporting security capabilities can (and should) be implemented as separate systems providing an enterprise level capability, these enterprise capabilities must be invoked (utilized) by the rest of the NAS.

Because security is not a single monolithic function, the SWIM security architecture cannot be addressed in isolation. In some cases SWIM will provide security controls that may be utilized by other entities in the NAS, while in other cases SWIM will rely on security controls provided by other systems or capabilities. Therefore, this section addresses the SWIM security architecture within the larger context of security in the NAS.

5.6.2 Drivers

Drivers for the SWIM ISS Architecture include:

- The overarching NAS Security Architecture
- Security needs identified in the analysis of NextGen midterm concept of operations
- FAA ISS Policies and Processes

Each of these drivers is described below.

5.6.2.1 NAS Security Architecture as a SWIM ISS Driver

The primary driver for the SWIM security architecture is conformance with, and support to, an overarching NAS Security Architecture. The NAS Security Architecture is currently under development as part of the NAS Enterprise Architecture. Appendix B provides a summary of the NAS Security Architecture, based on the current state of the NAS Security Architecture work being performed by MITRE/CAASD in support of the FAA at the time of this writing. This section provides a brief summary of the major capabilities included in this architecture, and discusses how each of these capabilities drive the SWIM architecture; that is, the implications of each capability area on the SWIM architecture.

Information Technology (IT) Infrastructure. This consists of wide area and local area network infrastructure that provides network connectivity within the NAS, as well as other IT capabilities such as Data Storage. This includes not just IP WAN connectivity from service delivery point (SDP) to SDP, but also the full suite of IP-related capabilities such as DNS and NTP. The SWIM security architecture assumes that a robust IT infrastructure will exist in the Segment 2 time period.

Identity and Key Management Infrastructure. This includes capabilities for managing a PKI and managing information about identities of NAS operators (humans) and systems (devices). At a minimum, device and user identity and key management capabilities are assumed to be available for use by SWIM core and by SIP systems. This SWIM architecture relies heavily on the existence of this infrastructure. More sophisticated capabilities (single sign-on, centralized policy decision point) may or may not be available in SWIM Segment 2.

SOA Infrastructure. This consists of the SWIM core components (hardware and software), as well as SIP-provided components, that implement the SOA core services functions of the NAS Enterprise Services functional architecture. Subsequent sections will describe the security controls that are included in the SWIM architecture associated with the SOA infrastructure, and how the SOA infrastructure can be used to facilitate aspects of the NAS Security Architecture, in particular boundary protection and internal policy enforcement.

External Boundary Protection. This includes controls to protect connections and information flows between NAS and non-NAS entities. The external boundary protection concepts in the emerging NAS Security Architecture have the following major implications (drivers) on the SWIM security architecture:

All SWIM information flows must pass through an enterprise-level NAS boundary protection zone and be subject to a set of controls applied at the boundary.

SWIM must support creation of application-layer guard gateways for NAS mission services, support services, and interaction services.

Internal Policy Enforcement. A key principle of the emerging NAS Security Architecture is that the NAS must be divided into enclaves, and that information flows crossing from one enclave to another must be subject to controls to ensure that only authorized (non-malicious) traffic is allowed to flow. These concepts in the NAS Security Architecture create the following drivers on the SWIM architecture:

SWIM must provide capabilities to control which NAS end systems are allowed to access services from other enclaves, and to control which information is allowed to flow among different NAS internal enclaves.

Incident Detection and Response. This area includes instrumentation (e.g., network sensors and host based sensors) within the NAS to collect information that may indicate an intrusion or other security-related incident is happening, capabilities to monitor, analyze, and correlate this information, and capabilities to coordinate an effective response, including correcting the problem as well as performing activities such as auditing, reporting and forensics analysis. These concepts in the NAS Security Architecture imply creation of the following drivers on the SWIM architecture:

SWIM components (both SWIM-core and SIP-provided) must be instrumented to provide incident detection visibility to the central monitoring, analysis, and correlation facilities (e.g., Cyber Security Management Center (CSMC)). This includes both network-based sensors, and also potentially feeds of host-generated logs and audit information.

SWIM support systems must provide for coordination with central incident detection and response entities (e.g., CSMC and SIG) to respond to security incidents.

Certified Software Management. This consists of a capability to provide approved software and patches, and to allow these to be distributed for use throughout the NAS in a secure manner. The implications on the SWIM architecture are:

Distributions of SWIM software (for both the SWIM core and SIP-provided components) must be signed by a NAS entity with the authority to approve software for use within the NAS.

Processes must be included in SWIM service provisioning and SIP and SWIM Core support operations to ensure that SWIM software is properly signed before deployment.

5.6.2.2   NextGen Midterm Concept of Operations as a SWIM ISS Driver

In (Prabhu and Thomson March 2009) MITRE/CAASD performed a notional analysis of the functions that might be needed to support eight of the OIs identified in (Boan and others September 2008). This preliminary analysis, based on a notional concept for how functions to support the OIs might be allocated to NAS systems, identified a set of needed security functions, including the need to perform boundary protection, identification and authentication, and authorization.

5.6.2.3   FAA ISS Policies and Processes as a SWIM ISS Driver

In Segment 2, this architecture assumes that SWIM will begin deploying SWIM Core components into the NAS in order to begin implementing a net-centric infrastructure. For this, SWIM will need to execute the FISMA-NIST-based FAA-ATO Certification and Authorization (C&A) process to achieve an acceptable level of risk

As in Segment 1, SIPs will continue to be responsible for securing NAS systems, and may need to perform SCAP updates. However, the SIP C&A process should be considerably simplified by the existence of an overarching NAS Security Architecture, as well as the ability to offload security requirements to elements of this architecture such as a NAS External Boundary Protection System and Identity and Key Management Infrastructure.

Resources available to SWIM and the SIPS to ensure risks are managed in accordance with FAA policy include:

- ATO C&A Templates

- National Institute of Standards and Technology (NIST) FISMA Documents

- NIST SP 800-95 Guide to Secure Web Services

- SWIM Final Program Requirements (FPR)

- SWIM Services Specification Document (SvSD)

- This SWIM Core Architecture document, in particular this section describing the general approach to security within the SWIM architecture.

5.6.3   Analysis

This section describes a set of security capabilities, applied at different points in the architecture, which together can meet the needs implied by the above drivers. Figure 5-20 shows the following five different areas of security capabilities, overlaid on the high level architecture:

1. NAS Enterprise ISS Capabilities

2. Boundary Protection ISS Capabilities

3. SWIM Core ISS Capabilities

4. NAS End System ISS Capabilities

5. Registry Controls
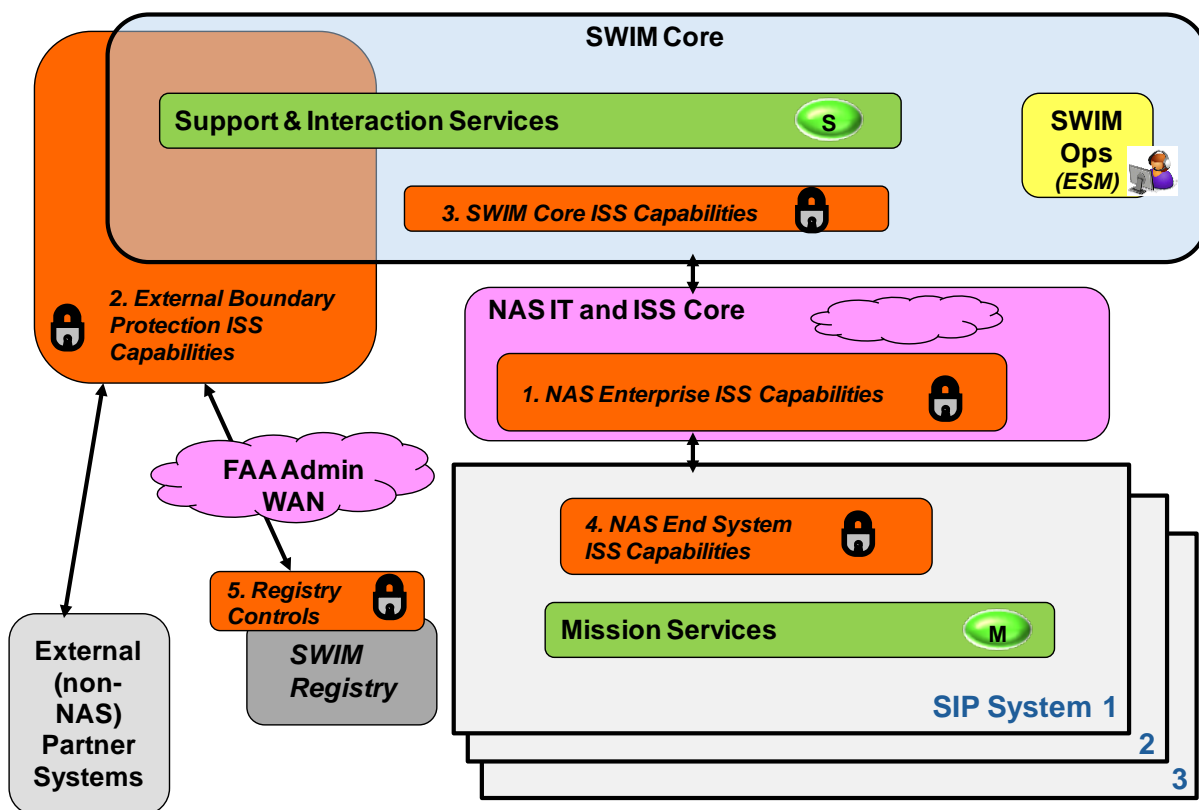
Figure 5-20. SWIM Security Capability Groupings

The security controls that make up each of these capabilities are discussed in the following sections.

5.6.3.1   NAS Enterprise ISS Capabilities

Grouped into this area of the SWIM architecture are ISS-related capabilities that are provided as part of an underlying IT/ISS infrastructure for use by systems throughout the NAS.

The capabilities in this area may be fully or partly allocated to programs other than SWIM in the Segment 2 time frame. For example, the Identity and Key Management Infrastructure may be allocated to a future segment of the LAACS program. Nevertheless, these items are essential parts of the larger SWIM architecture, and their security characteristics and capabilities are essential for SWIM security.

The capabilities, described in more detail in Appendix B, include:

- Secure IP network transport

- Identity and Key Management Infrastructure, including capabilities for managing keys and identity information for the NAS

- Intrusion Detection and Response, including central monitoring, analysis, and correlation, as well as coordination of response actions

5-49

5.6.3.2   Boundary Protection ISS Capabilities

This area includes a range of controls applied to connections and information exchanges between the NAS and external (non-NAS) entities. These include network layer controls (e.g., VPNs, firewalls) as well as application layer controls (guard gateways, which break the connection between NAS and non-NAS systems, and inspect the application data content to ensure that it conforms with predetermined rules before allowing it to pass). At the time of this writing, responsibility for implementing these controls in the Segment 2 time frame has not been clearly allocated to different programs, but we can make some reasonable assumptions. In this document we assume that the FTI program, having already made considerable progress in implementing NAS Security Gateway services (based on ED-8), will provide network layer controls. (Network layer controls are not discussed further in this document.) Since application layer controls are, by definition, dependent on the nature of the application and type of information that is flowing, NAS programs that have applicable domain knowledge must have a role in developing and operating the application layer controls. However, even though the information content may vary for different NAS programs, SWIM-compliant information flows will be built using a limited set of standardized protocols. This makes it possible to use a common set application layer security controls. It will be simpler and ultimately more effective to use a common set of application layer controls rather than to build a unique solution for each program. Therefore, we assume that, for SWIM applications in Segment 2, application layer controls will be built to meet the needs of SIPs using a common set of SWIM core boundary protection capabilities, operating within a set of network controls that provide a NAS Exterior Boundary Protection System.

5.6.3.2.1   General Architecture for Exterior Boundary Protection

Figure 5-21 provides an overview of this concept, showing a NAS System communicating with an external entity via an application gateway operating within the External Boundary Protection System. Since the application gateway must implement system-specific functionality, this architecture has implications on how the systems must be operated and supported. As shown in the figure, NAS operational personnel that have the local knowledge and responsibility for supporting the operations of a specific NAS system must have processes and tools that allow them to define the policies, rules, and domain-specific logic to be enforced by the gateway. The External Boundary Protection System and/or SWIM operational personnel are assumed to operate the External Boundary Protection System infrastructure and security controls. External Boundary Protection System/SWIM operational personnel and NAS facility/system operational personnel must both be involved in monitoring and responding to performance issues, faults, or exceptions.
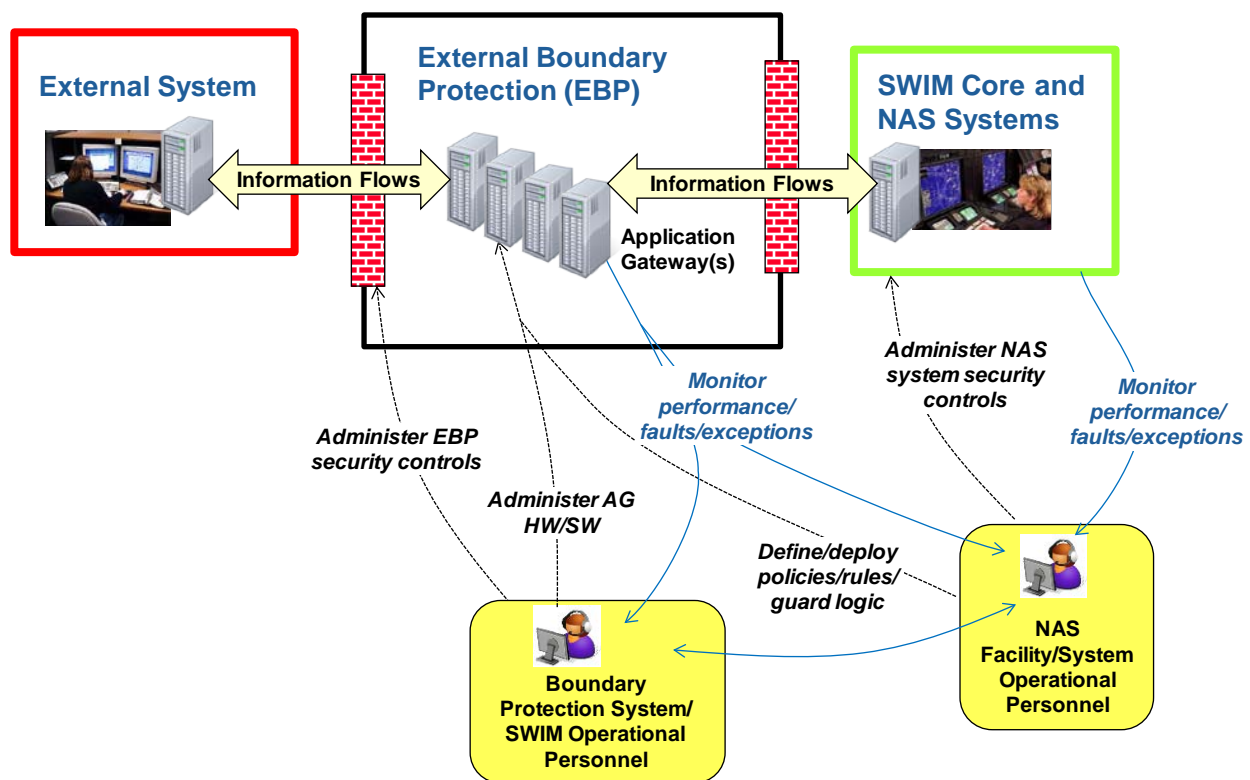
Figure 5-21. General NAS External Boundary Protection Concepts

Application layer protections for different types of SWIM information flows are discussed in the following subsections. (Legacy information flows which do not conform to SWIM standards are also included in the External Boundary Protection System concept, but are not discussed here.)

5.6.3.2.2   SWIM Boundary Protection for Interaction Services

In SWIM Segment 2, Interaction Services may be made available to non-NAS entities using web protocols (HTTP and HTTPS) carrying content to be presented to the user within a browser. This may include simple Hyper Text Markup Language (HTML) content, as well as many varieties of dynamic web content, including RSS feeds for web-based notification services. (Content such as SOAP messages intended for machine processing rather than rendering in a browser, is not included here, but is discussed below.)

The capabilities necessary for protecting this type of service are described in (NIST September 2007).

Interaction services include services intended for the general public, for which no identification is required, as well as services intended for aviation partners, for which user identification and authentication and authorization is required. Both types of interaction services are discussed below.

Figure 5-22 shows a notional boundary protection concept for Interaction Services for the general public. As shown in Figure 5-22, an unidentified user, using a standard web browser,

5-51

connects over an external network to retrieve content and interact with an FAA-provided NAS service. The externally visible web server that the user's browser connects to is actually a reverse proxy web server, which can perform monitoring and filtering of HTTP content, before passing the HTTP operations on to the actual web server. We assume the existence of reverse proxies based on the guidance in NIST SP 800-44v2. However it is not the intent of this document to specify the design of NAS boundary protection systems, so this diagram should be taken as notional. Other designs are possible, and any specific details discussed in this document should be taken as examples, not specifications.

If the content provided by the interaction service was relatively static, then it might be possible for this content to be manually loaded onto the server by administrators. However, in general, the interaction service information content must be dynamically obtained from, or provided to, systems within the NAS. To accomplish this, the web server in the External Boundary Protection system must be able to use the NAS WAN to access Mission Services and Support Services in the interior of the NAS. As shown in the figure, this is accomplished by connecting to these services over the NAS WAN, subject to additional controls that protect these internal services, which are discussed in subsequent sections.
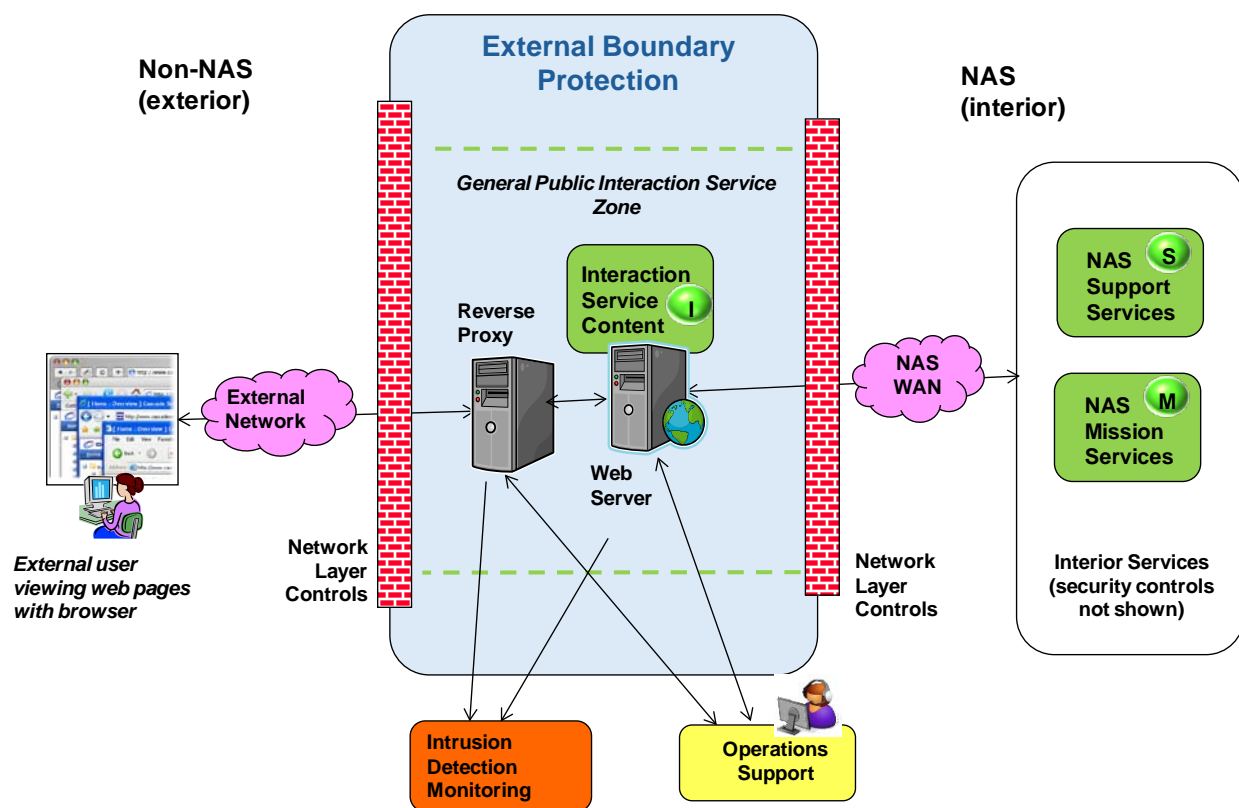

Figure 5-22. Notional ISS Controls for General Public Interaction Service

Up to this point we have addressed interaction services that are available to the general public, for which no identification or authorization is performed. In order to provide more general interaction services for NAS partners, we need to add mechanisms for identification and

5-52

authentication (I&A), and authorization. A notional set of controls for this is shown in Figure 5-23. Most of the components are the same as previously discussed. The user still accesses web content from an externally visible URL, but the web interface must include authentication of the user's identity, and may also include encryption to ensure confidentiality and integrity. There are different mechanisms that may be used for this, including:

- Username and password over HTTPS

- X.509 certificates over HTTPS

- Security Assertion Markup Language (SAML) assertions over HTTPS

Analysis of which combination of these will be utilized in SWIM Segment 2 is beyond the scope of this document. Here we assume simply that, after receiving credentials from the user, the reverse proxy server uses the Identity and Key Management Infrastructure to authenticate the user's identity. This may include checking that a user's certificate has been signed by a trusted authority, as well as checking against a Certificate Revocation List (CRL) or using an On-Line Certificate Status Protocol (OCSP) responder to make sure the user's certificate has not been revoked.

Continuing the analysis of Figure 5-23, once I&A has been accomplished, an authorization decision remains to be made. This decision could be made locally within the reverse proxy based on local configuration rules or access control lists that defined which users are allowed to access which pages. However, a solution based on local configuration is only manageable for a limited number of applications and users; this type of solution does not scale well. Therefore, we assume that the reverse proxy server again relies on the Identity and Key Management Infrastructure for authorization. For this the Identity and Key Management Infrastructure will provide a Policy Decision Point that may be queried to determine whether to grant access for this user to the requested resource. For example, eXtensible Access Control Markup Language (XACML) could be used to define the access control policies, and SAML could be used across the network to allow the Policy Enforcement Point (PEP) to query the Policy Decision Point (PDP). If the PDP approves access, the request is propagated to the actual web server, and the information flow continues as in the previous example; if not, access is denied.

Once authorization has been completed, user access to the web content is provided. As discussed above, this web content may be built using mission and support services provided from within the NAS, subject to additional controls that protect the internal services, discussed in subsequent sections. Note that these additional controls may also require access to the identity and key management infrastructure.
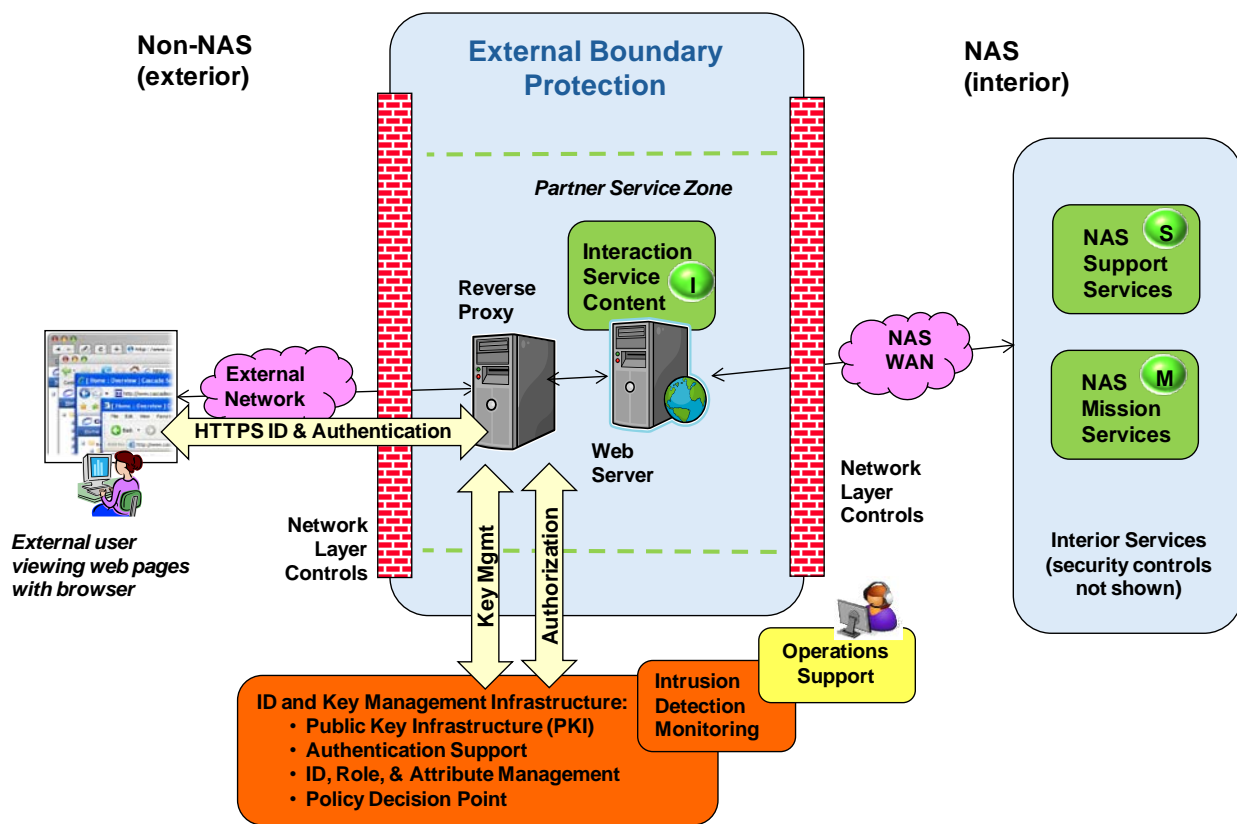
Figure 5-23. Notional ISS Controls for Partner Interaction Services

5.6.3.2.3   SWIM Boundary Protection for Support Services

While interaction services interface more or less directly with a human user (for example, a NAS facility status display that a user might view using a browser), support services are intended for further processing by an external system (for example, NAS status messages ingested into an airline's flight planning automation system). According to SWIM standards, the information content will be exchanged between the partner system and the FAA in the form of XML messages, which are encapsulated in a SOAP envelope. The SOAP envelope containing the XML messages may be transported over HTTP or JMS, which in turn may be transported over a SSL. The XML content of the message may be encrypted and signed, as indicated in the SOAP header in accordance with WS-Security standards.

Boundary protection for externally visible Support Services is conceptually similar to the mechanisms discussed above for Partner Interaction Services, but there are differences due to the protocol difference and also due to the fact that the FAA is not providing services directly to an individual user, but rather to another system. The architecture is shown in Figure 5-24.

Figure 5-24 shows a partner system interacting with FAA-provided support services made available from a SWIM Core ESB/Messaging platform within the External Boundary Protection System, protected by an XML gateway appliance. Again, it is not the intent of this document to specify the design of NAS boundary protection systems, so this diagram should be taken as

5-54

notional. However, the use of XML gateway appliances to protect externally visible web services would be an essential part of any solution. As stated by NIST:

"Because XML Schemas can rigidly define the types of data and format of XML elements, they can be used to prevent the Web service from processing invalid requests… Use of XML Schema-based access control could prove to be more powerful than programmatic access control since many malicious SOAP requests would not reach the application code." (NIST August 2007)

In addition to schema checking, the XML gateway may also provide enhanced performance and may be used to support I&A and authorization processing.

I&A between the partner system and the FAA may be done on a session basis (using credentials passed over an HTTPS connection), on a per-message basis (using credentials passed in the SOAP header), or both. Authentication may performed on the identity of the partner system, the end user accessing the partner system, or both. For all of these cases, the XML gateway will rely on key management and authentication capabilities provided by an Identity and Key Management Infrastructure.

Once I&A has been completed, an authorization decision must be made. As with interaction services, this could be performed using locally configured information within the XML gateway or ESB platform. However, such solutions cannot be easily scaled up to support many users and many applications. Therefore, we assume that the XML gateway (or ESB platform) will rely on a policy enforcement point provided by the Identity and Key Management Infrastructure to make an authorization decision.

In order to support dynamic content, externally visible support services provided by a SWIM Core ESB platform within the External Boundary Protection system may need to be dynamically built by accessing NAS internal support services. This is done by XML message exchange with the internal SWIM Core ESB platform, subject to additional controls not shown here but discussed in subsequent sections.
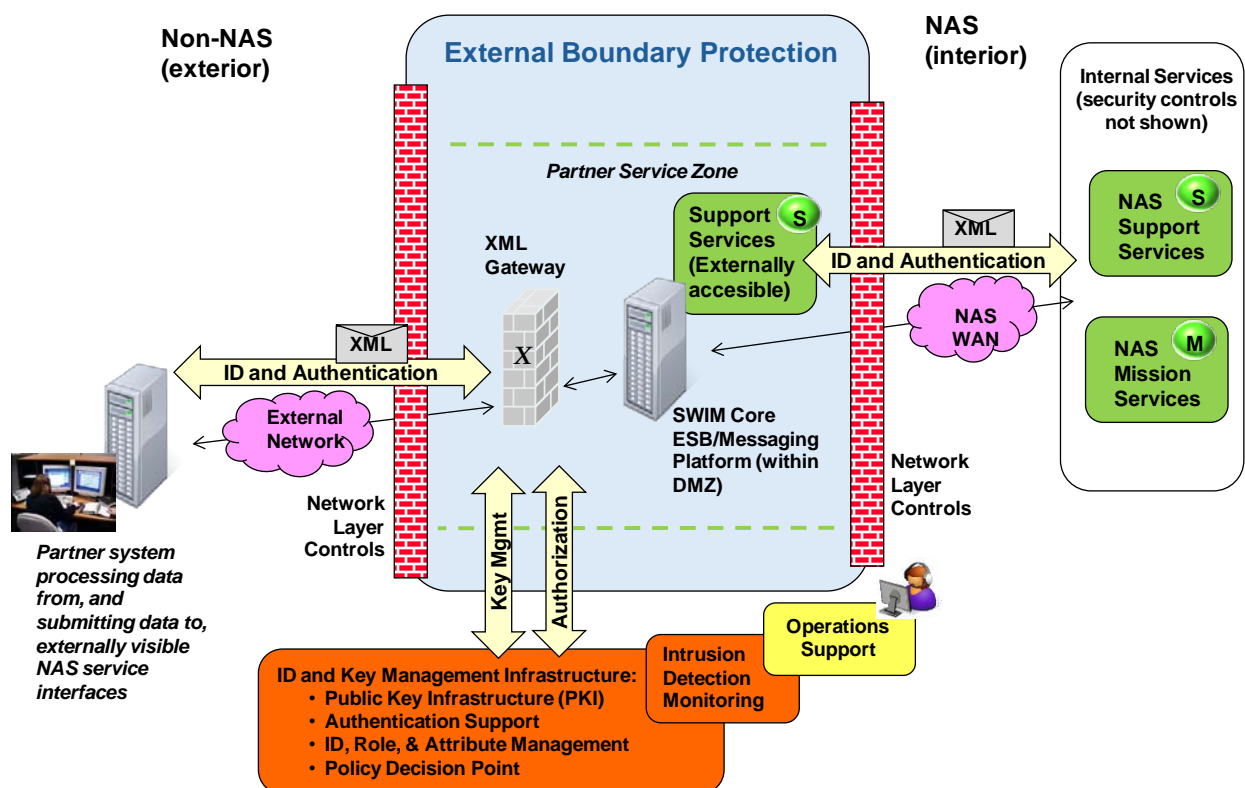
Figure 5-24. Boundary Protection Mechanisms for Support Services

5.6.3.3   SWIM Core ISS Capabilities

The details of the security controls necessary to protect the SWIM Core are beyond the scope of this document, and will require a thorough analysis as part of a C&A process in accordance with (FAA Order 1370.82A, Information Systems Security Program September 2006) and (FAA, Information Security Certification and Accreditation (C&A) Package March 2008). However, for the purposes of defining the general structure of the SWIM architecture, some general conclusions can be drawn about the need for controls to protect the SWIM core, and what the general nature of these controls must be.

There are two considerations that lead to the conclusion that additional controls will be needed to protect the services and systems within the SWIM core.

The first consideration is that systems and services within the SWIM Core will need to be accessed from platforms within the External Boundary Protection system, in order to make possible information exchanges with aviation partners and the general public. As discussed above, the External Boundary Protection concept will prevent SWIM Core systems and services within the interior of the NAS from being directly accessed and attacked by non-NAS entities. However, despite our best efforts to protect them, we must consider the possibility that web servers or ESB platforms within the External Boundary Protection System may be attacked and compromised and then serve as a vector for attack on the internal functioning of NAS. To

5-56

prevent this, additional security controls must be provided to protect services within the SWIM Core.

The second consideration is the enclave concept that is part of the emerging NAS Security Architecture. In order to prevent a security compromise within the NAS from spreading in an uncontrolled manner, the SWIM Core should be considered a separate enclave, and application layer protections applied to information flowing into or out of the SWIM core.

While it would be premature to state the details of the security controls needed to protect the SWIM core, at a very basic level we see the need for network level protections, as well as additional application layer protection. Network level protections are not discussed here; rather we focus on application layer controls.

In all but the most limited options for the SWIM Enterprise Messaging Bus architecture, the SWIM Core hosts Support Services and Interaction Services for NAS internal use. Some of these services may be made available for any other NAS system or user to access, however we assume that for the majority of services (perhaps all), I&A and authorization will be required. These operations may be performed at the session level, the message level, or both. I&A and authorization at the session level (for example, using symmetric HTTPS authentication) can be performed using the identities of the peer systems. For example, in the case of a ESB platform in the External Boundary Protection System accessing SWIM core services, I&A and authorization at the session level would be based on the identities of the SWIM Core ESB platforms in the External Boundary Protection System and in the interior of the NAS. I&A and authorization may also be performed at the message level, if needed by the particular application (for example using information in a SOAP message header encoded in accordance with the WS-Security standards). I&A at the message level is more flexible, and may be done using the identity of the original service requestor (e.g., the NAS partner system or user of the NAS partner system). Again, the capabilities of the Identity and Key Management Infrastructure (e.g., key management, authentication support, policy decision support) may be utilized to ensure a scalable and manageable solution.

An overview of these capabilities is shown in Figure 5-25. As shown, the SWIM Core contains ESB platforms hosting support services, and web server platforms hosting interaction services. These services may be accessed from the External Boundary Protection System (for information exchanges with the public and with partners) and from SIP systems (for information exchange with NAS systems, controllers, flow managers, and support personnel). The SWIM Core ESB platforms and web server platforms will be isolated behind proxy devices such as XML gateways and reverse web proxies. As described above, I&A of systems and users may be performed by these "front end" gateway devices, using the capabilities of the Identity and Key Management Infrastructure.

Other security functions such as confidentiality and integrity between the SWIM core and other systems may also be provided at a connection level (using HTTPS) or at a message level (using XML encryption and WS-Security).

5-57

In order to provide intrusion detection and response capabilities, the SWIM core will be instrumented with sensors (potentially both host and network based) that feed data to a central monitoring, analysis, and correlation facility, as shown in Figure 5-25.
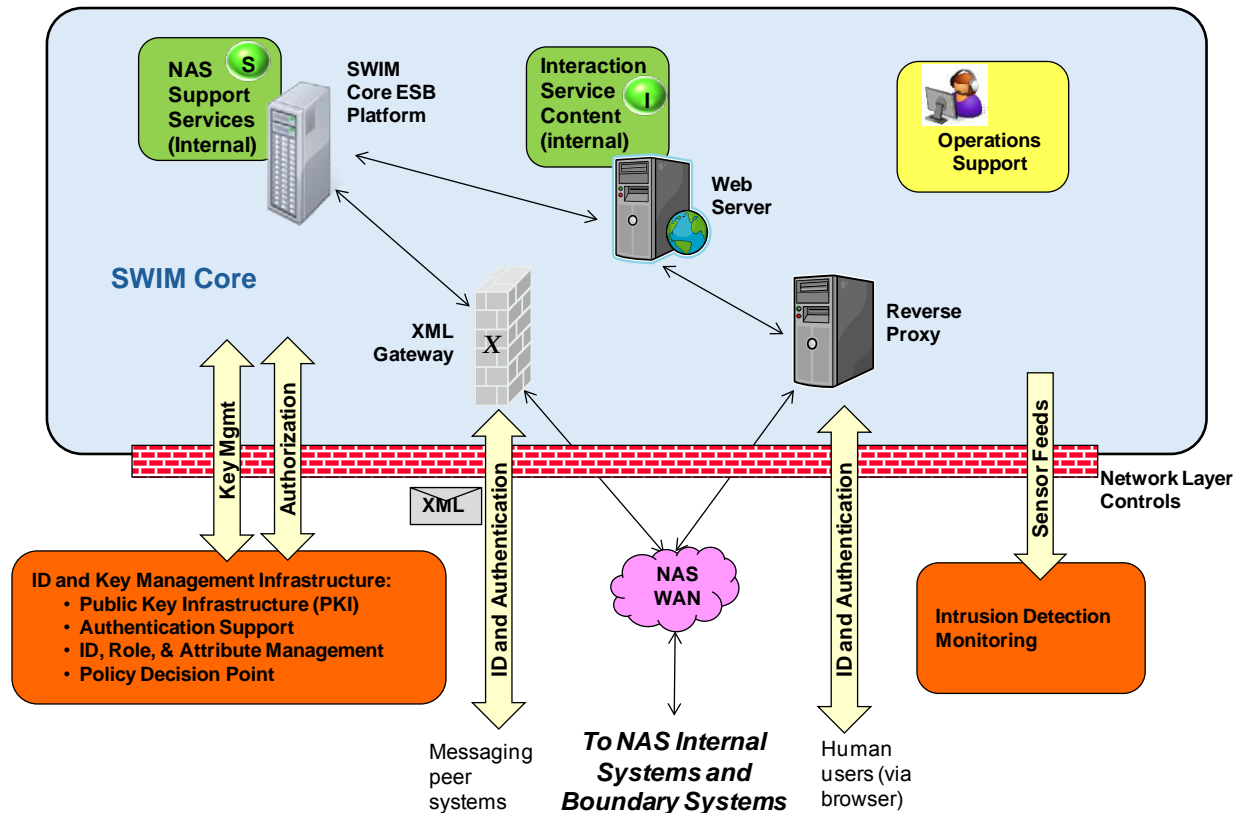
Figure 5-25. SWIM Core ISS Capabilities

In addition to the architectural features described above, additional controls will be needed to protect the platforms and data within the SWIM Core. For example, operating systems should be patched, unused services disabled, unused ports and protocols closed, and so on. NIST 800-53 contains a full discussion of the range of security controls that may be needed.

5.6.3.4   NAS End System ISS Capabilities

As with the SWIM core, the details of the security controls that will be needed by each NAS system are beyond the scope of this document, and will be determined as part of the requirements analysis and C&A process for these systems. However, we can discuss some of the general architectural features of NAS end system security as it relates to the SWIM architecture.

A notional example of NAS end system security controls related to SWIM, for a system which required a relatively high level of security, is shown in Figure 5-26. This example assumes that the NAS end system is providing Mission Services via the NAS WAN. These services may be consumed by other services within the SWIM Core, or directly by other NAS systems. The NAS System may also be receiving messages, or consuming services, from the SWIM Core or from

5-58

other NAS systems. The example assumes that the NAS system has deployed some form of application layer gateway (shown as an XML gateway in the figure) to perform checking of data flowing into or out of the system, as well as to off-load I&A and authentication processing. This processing is in turn supported by capabilities in the Identity and Key Management Infrastructure. The XML gateway, or logic within the SIP ESB platform, or even possibly within the legacy NAS system may perform application-specific or fine-grained access control that augments access control mechanisms provided within the SWIM core or within any NAS boundary protection systems.

The figure also show feeds from host and/or network based sensors within the SIP that are provided to a central intrusion detection and monitoring facility (e.g., CSMC).
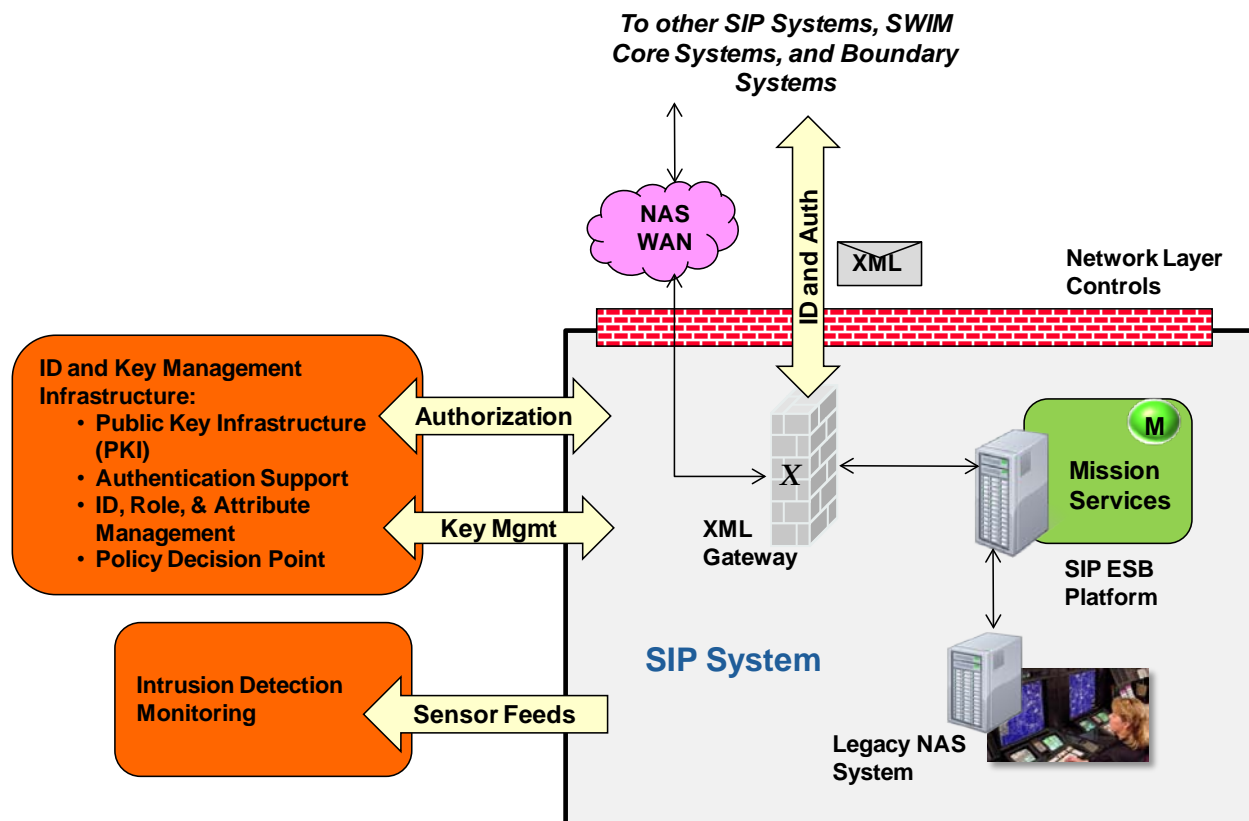
Figure 5-26. Notional NAS End System Security-Notional High Security Example

Another notional example of NAS end system security controls related to SWIM is shown in Figure 5-27. In this example, a set of end systems X_1, X_2, … X_N, that have some degree of mutual trust have been grouped into an "enclave", and some of the security requirements for the enclave have been allocated to the network provider and the SWIM Core. The network provider (e.g., the FTI Program) provides a set of network layer controls that allows the systems within the enclave to access each others' end points, and the SWIM Core is also connected to the

enclave[4]. This allows the systems within the enclave to freely access each other's services, and to access services in the SWIM Core, as well as allowing the SWIM Core to receive information from systems within the enclave. However other systems (e.g., systems implemented by SIP Y, as shown in the figure) have no direct network connectivity to the enclave. Systems that are not part of the enclave can only exchange information with systems in the enclave by passing through the SWIM Core, where additional security controls can be applied. For example, the SWIM Core may use security controls to enforce policy that allows only specific systems to access information from enclave X. It may also check format and content of information being provided to enclave X to ensure that it is legal, thereby blocking potential malicious content.
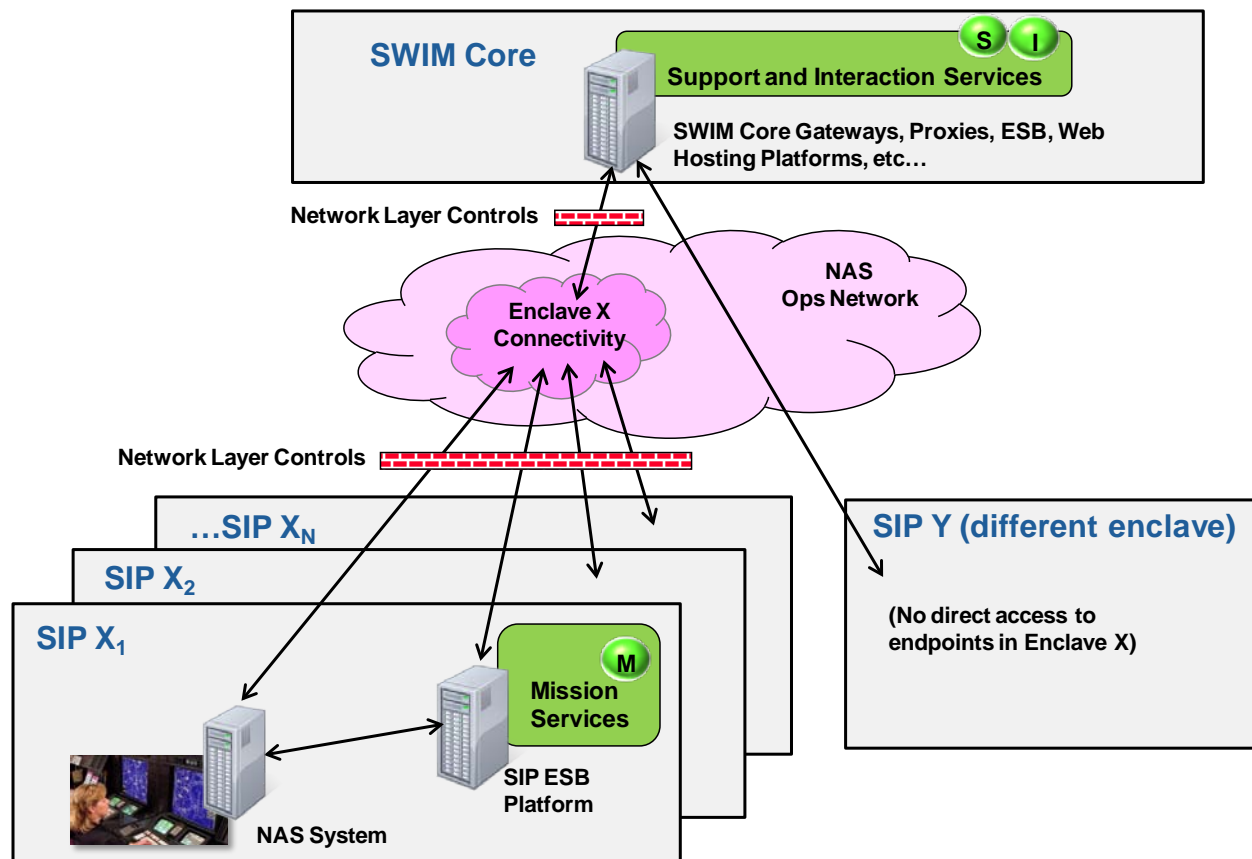
Figure 5-27. NAS End System Security – Enclave Example

It is important to realize that the enclave concept illustrated in Figure 5-27 does not obviate the need for SIPs to consider security requirements. It allows SIPs to allocate some security requirements to the net centric infrastructure provided by the network provider and the SWIM Core, but some security requirements are likely to continue to be allocated to the end system. For example, the end system may still have requirements to identify and authenticate users logging onto the system locally, to collect logs for audit processing, provide physical security, and so on.

---

[4] Various proven designs are possible for implementing the enclave concept within the network, including link layer solutions, virtual LAN (VLAN) solutions, or virtual private network (VPN) solutions.

Underlying infrastructure (e.g., identity and key management infrastructure) may be available to facilitate meeting these end system requirements, but the NAS end system will still be responsible for invoking the infrastructure services to perform these functions.

5.6.3.5 Registry Controls

Read access to the SWIM registry is necessary for users to discover what services are available and how to access those services. This information could potentially be used by a malicious entity to discover possible vulnerabilities, as part of pre-attack reconnaissance. Write access to the SWIM registry must also be provided to allow service information to be published. This access could be abused (accidentally or deliberately) to corrupt the information in the registry. To mitigate these risks, the registry must implement access control to ensure that only authorized users are able to discover and publish information. Discovery should be limited to the minimum information necessary. The Identity and Key Management Infrastructure can again be utilized to provide these controls in a scalable manner.

Other controls will also likely be needed, including basic measures such as hardening the operating system platform hosting the registry, having different instances of the same registry for staging and production, and so on. These controls will be identified as part of the registry C&A process.

5.6.4 SWIM Security Assumptions and Options

In this section we first present assumptions and options in each of the areas discussed above; then we combine and summarize the options into a set of overall security options for the SWIM architecture.

5.6.4.1 NAS Enterprise ISS Capabilities Assumptions and Options

We consider most of the capabilities in this area to be essential; if they are not implemented by other programs, they will need to be implemented by SWIM. Therefore, we assume that these capabilities are present in any architecture option selected for SWIM segment 2, as summarized in Table 5-13. However, there are options in the extent of functionality that is included in the Identity and Key Management Infrastructure capability area. While there are potentially a large number of different degrees of capability that could be considered, we consider two options: a basic capability and a full capability, as shown in Table 5-14.

Table 5-13. Assumptions Related to NAS Enterprise ISS Capabilities

Assumption	Description	Rationale
ISS-ENT-A1: Secure IP network transport	A secure IP network (including complete set of IP network services such as DNS and NTP) is provided and operated by a single provider for the entire NAS.	FTI already provides IP WAN transport for the entire NAS. Net-centric capabilities are not possible without a robust and complete network infrastructure.
ISS-ENT-A2: Enterprise Intrusion Detection and Response	Intrusion detection sensors (host and network-based) are deployed where needed throughout NAS, including throughout SWIM core and SIP systems, with a central monitoring and analysis capability (e.g., CSMC). Also assumed is central coordination of a NAS response capability (e.g., CSMC working together with the NAS Security Information Group (SIG).	Required by the NAS Security Architecture.

Table 5-14. Options Related to NAS Enterprise ISS Capabilities

Option	Description	Pros/Cons
ISS-ENT-O1: Limited Identity and Key Management Infrastructure	In this option, only a limited set of capabilities are provided as part of a NAS-wide Identity and Key Management Infrastructure, including capabilities to issue keys for devices and humans, for use throughout the NAS, as well as support for authentication of keys.	Pros • Higher confidence that simpler Identity and Key Management Infrastructure capability can be fielded quickly Cons • User identities (accounts) must be administered for each program and application • Authorization rules must be administered for each program and application • Does not scale well

Option	Description	Pros/Cons
ISS-ENT-O2: Complete ISS Support Infrastructure	A robust Identity and Key Management Infrastructure is provided that supports all of the capabilities described above.	Pros • Can be scaled up to large numbers of applications and users • Economies of scale and centralization of expertise can lead to lower total cost and a more robust and secure solution overall Cons • Increased cost and technical and schedule risk to the Identity and Key Management Infrastructure implementing program (May be mitigated by success of LAACS program for non-NAS systems)

5.6.4.2   Assumptions and Options Related to External Boundary Protection

The assumptions in this area are shown in Table 5-15. In this area, there are two major options, which boil down to whether SWIM or some other program (e.g., FTI) will provide a common set of capabilities to be used by all SIPs, or to let SIPs invent their own solutions to operate within a common set of network layer External Boundary Protection controls. These SWIM architecture options for boundary protection are summarized in Table 5-16.

Table 5-15. Assumptions Related to External Boundary Protection

Assumption	Description	Rationale
ISS-BP-A1: External Boundary Protection System	External Boundary Protection System that provides the network layer protections for the NAS boundary, within which application layer protections for specific NAS services must be placed.	NAS Security Architecture decision.

Table 5-16. SWIM Architecture Boundary Protection Options

Option	Description	Pros/Cons
ISS-BP-O1: No common application gateway support	SIPs implement their own application gateway solutions within a common External Boundary Protection System.	Pros • Less cross-program dependencies • Programs can implement solutions tailored to their requirements Cons • Increased development costs due to duplication of effort

Option	Description	Pros/Cons
		• Increases the complexity of operation of the External Boundary Protection System, due to the need to accommodate a variety of different solutions • Difficult to assess overall security
ISS-BP-O2: Common Application Gateway services for Boundary Protection	SWIM deploys a common set of capabilities (e.g., reverse proxies, XML gateways, web server platforms, and ESB platforms for hosting Interaction Services and Support Services capabilities within a External Boundary Protection System, to be used by all SIPs).	Pros • More robust and scalable common security solution • Overall NAS solution will be much simpler and easy to assess • Simpler operation of External Boundary Protection System Cons • Greater cross-program coordination required

5.6.4.3 Security Assumptions and Options Related to SWIM Core Protection

In this area, while design choices remain to be made, we do not see any major architectural options. To the extent that SWIM Segment 2 includes NAS Support Services and Interaction Services, these services will need to be protected by network layer and application layer mechanisms similar to those shown in Figure 5-25. These assumptions are summarized in Table 5-17.

Table 5-17. ISS Assumptions Related to SWIM Core

Assumption	Description	Rationale
ISS-SC-A1: SWIM Core network layer protections	A set of network layer protections (e.g., firewalls) will be provided to isolate the SWIM Core systems.	Network layer protections prevent application layer protections from being subverted.
ISS-SC-A2: SWIM Core application layer protections	Devices such as reverse proxies and XML gateways provide application layer protection for Interaction Services and Support Services hosted in the SWIM Core.	Application layer security controls for internal policy enforcement are a key concept in the NAS Security Architecture.

5.6.4.4 Overall Security Options

To reduce the total number of options that must be considered, related sets of options are logically grouped together. The resulting overall options for ISS are summarized in Table 5-18.
.

Table 5-18. Summary of ISS Options

Option	Description	Pros/Cons
ISS-O1: Basic ISS core capabilities	A basic set of ISS capabilities are provided as a NAS enterprise resource. Identity and Key Management Infrastructure provides basic key management capabilities (ISS-ENT-O1). Network layer NAS boundary protection is provided, but no enterprise level capability is provided for application layer gateway (ISS-BP-O1).	Pros • Reduced risk and cost for SWIM and IT/ISS programs Cons • Increased total risk and cost for individual programs due to duplication of solutions • Increased overall complexity and reduced overall security • SIPs remain responsible for most security functions • Does not scale or evolve well
ISS-O2: NAS Enterprise Security in SWIM Core	A robust Identity and Key Management Infrastructure is provided; including full key and identity management and access control support (ISS-ENT-O2). Also, SWIM provides hosting services to provide a common application gateway environment for boundary and interior protection control. (ISS-BP-O2).	Pros • Can be scaled up to large numbers of applications and users • Economies of scale and centralization of expertise can lead to lower total cost and a more robust and secure solution overall • Security in SWIM Core supports all NAS end systems Cons • Increased cross-program dependencies and coordination • Increased cost and technical and schedule risk to the SWIM and Identity and Key Management Infrastructure implementing program (May be mitigated by success of LAACS program for non-NAS systems)

6 Overall Architecture Options and Recommendation

6.1 Overall Architecture Options

In the course of presenting the SWIM Architecture, various options have been presented in each area. In order to create a manageable number of overall options for the SWIM Program to consider we proceeded as follows. First, we included the option of continuing the Segment 1 federated approach. Next, we combined less complex and powerful options from each area to create Option 2. Finally, we combined the more complex and powerful options from each area to create Option 3. These three options are described and assessed in Table 6-1.

Table 6-1. Summary of Overall Options

Option	Description	Pros/Cons
Option 1: Federated approach	Continues the approach taken in SWIM Segment 1. SWIM core services are provided by SIPs within the bounds of NAS systems – only the SWIM registry exists as SWIM-provided infrastructure.	Pros • Minimal near-term risk and cost for SWIM and IT/ISS programs Cons • NAS remains tightly coupled and the infrastructure to enable and centralize shared information across NAS programs does not exist. The lack of such infrastructure reduces the ability to "on-ramp" information to a SWIM core. • Limited ability to apply common security solutions • No end-to-end service management
Option 2: SWIM Core Basic Messaging	The following options from each area are included: • EMB-O1: Only message brokers in the SWIM core, providing a messaging layer that can be utilized by SWIM Mission Services implemented by SIPs • WS-O1: No web hosting support • ISS-O1: Identity and Key Management Infrastructure limited to key management, SIPs implement their system-specific application layer boundary protection within common NAS External Boundary Protection System • ESM-O1: SWIM operations	Pros • Low near-term risk and cost for SWIM and IT/ISS programs Cons • Provides only limited "on-ramping" capability, with no support for any application layer services in the SWIM Core (no Support or Interaction Services) meaning that NAS continues to remain tightly coupled. • Limited ability to apply common security solutions • Only a minimal increment towards goal of net-centric NAS

Option	Description	Pros/Cons
	manages only the message brokers, no centralized service management • REG-O1: Basic registry with no interface to ESM	
Option 3: SWIM Core SOA Infrastructure	A combination of the following options from each area constitutes this option: • EMB-O2: Service construction capability - allows Support Services to exist in the SWIM Core • WH-O2: Web hosting capability allows Interaction Services to be deployed to SWIM Core • REG-O2: Registry and run-time service locator integrated with ESM • ESM-O2: Central fault and performance monitoring with a migration path to more advanced features such as SLA compliance checks • ISS-O2: ISS Support Services centralize key and identity management, and support authentication and authorization decisions. SWIM Core provides general purpose application layer solutions (e.g., XML gateway, reverse proxy) for Support and Interaction services	Pros • Allows "on-ramping" of information to NAS-wide services in the SWIM Core, providing greater opportunities for loose coupling between NAS programs • Can support rapid deployment of new NAS information processing functions in the SWIM core, allowing more rapid progress toward NextGen operational improvements • Puts in place NAS-wide solutions for security and support of the IT core, which can improve the overall security posture of the NAS and simplify security and support for new SIPs. • Allows some level of end-to-end service monitoring which will facilitate rapid troubleshooting to resolve problems Cons • Cost and technical risk (but these can be largely mitigated by adopting an evolutionary approach)

Option 1 consists of a continuation of the federated strategy used in SWIM Segment 1, as shown in Figure 6-1.
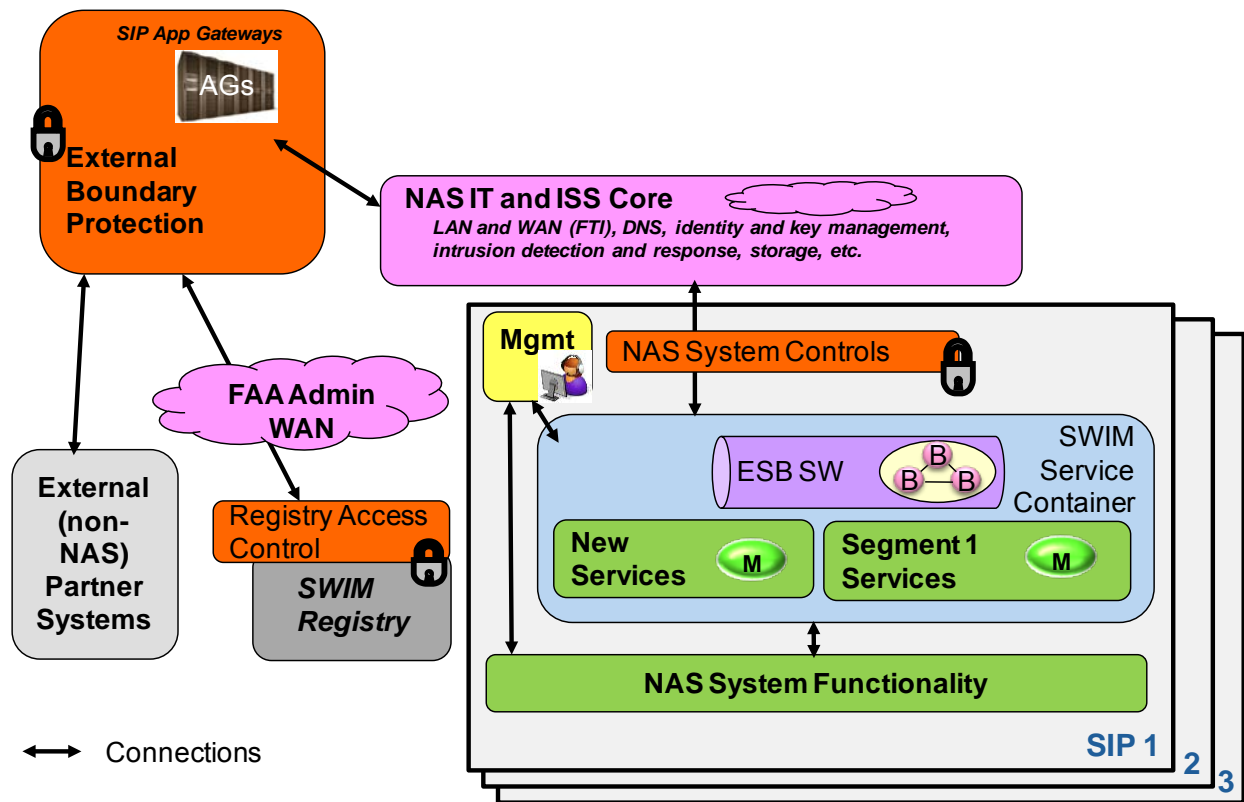
Figure 6-1. Overall Architecture Option 1

Option 2 is illustrated in Figure 6-2. In this option, SWIM implements messaging brokers in the SWIM Core, together with basic SWIM operations support. This option assumes only a basic Identity and Key Management Infrastructure exists to issue and manage keys for devices (e.g., server certificates). Note that in this option there is no provision to host NAS application level services (Support Services or Interaction Services) in the SWIM Core. Also, in this option, SIPs must implement application gateway functionality in the External Boundary Protection System.
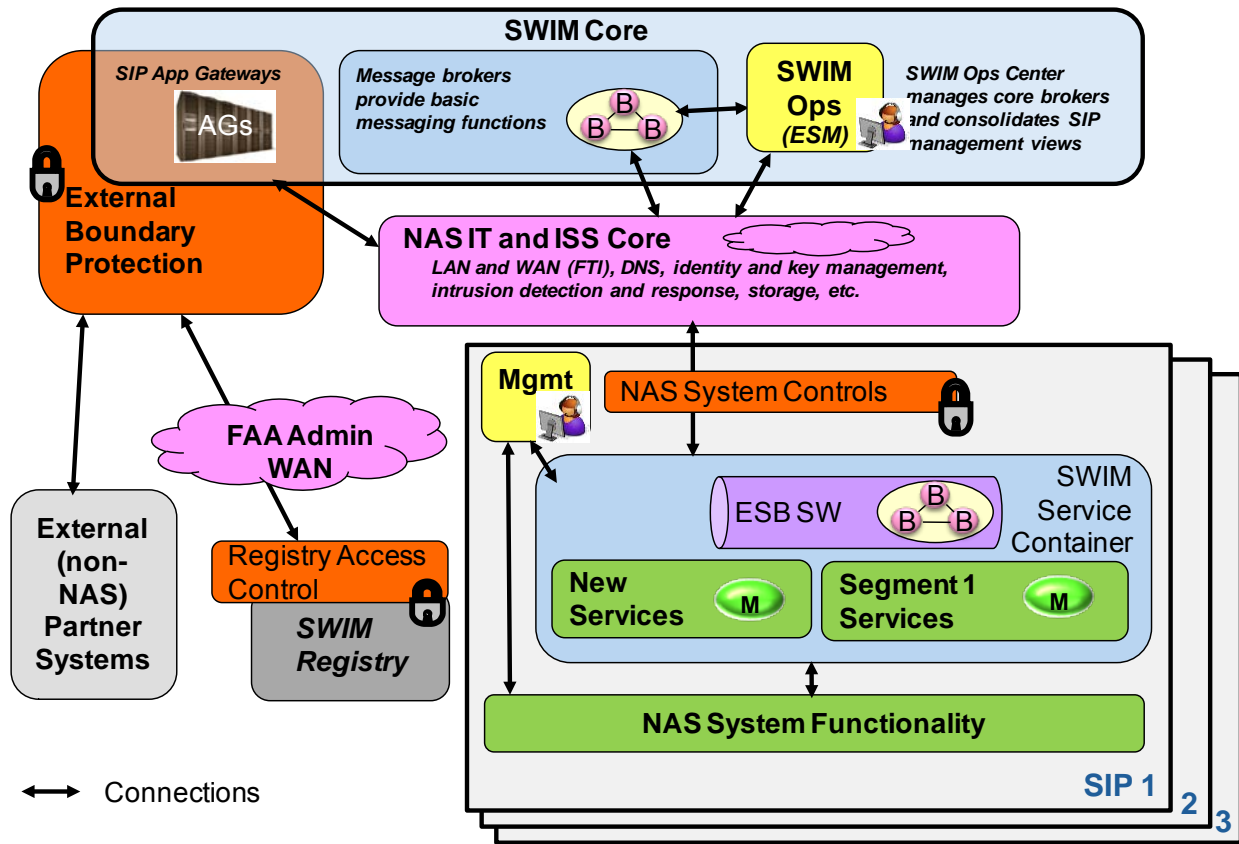
Figure 6-2. Overall Architecture Option 2

Option 3 is illustrated in Figure 6-3. This option allows Support Services and Interaction Services to be hosted in the SWIM Core. Clearly there are variations possible within Option 3 that differ in the degree of sophistication and integration of the ESB and ESM capabilities in the SWIM Core. The figure shows a full suite of capabilities in the SWIM Core, including ESB and web application hosting capabilities onto which Support and Interaction services can be deployed.
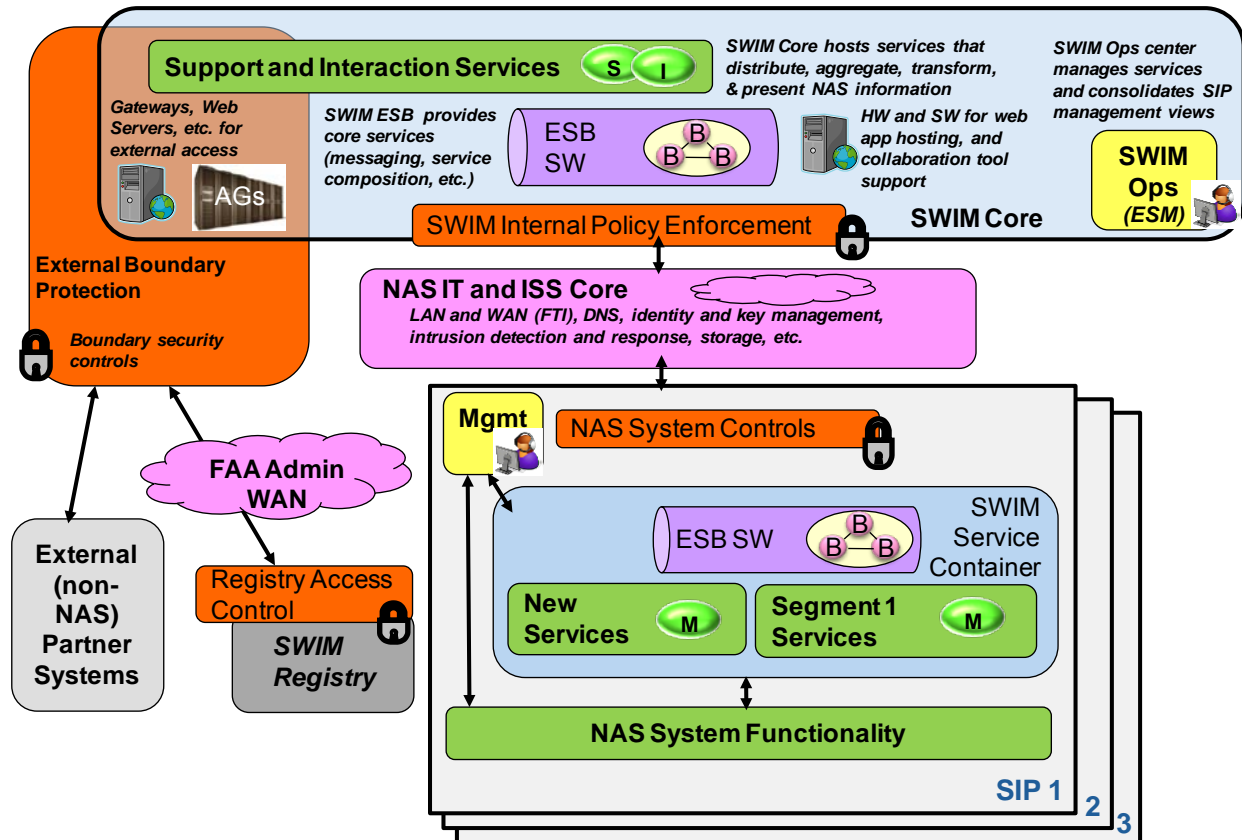
Figure 6-3. Overall Architecture Option 3

6.2   Recommendation

Given current knowledge, the FAA should select Option 3 for SWIM Segment 2, to be implemented in an incremental and evolutionary approach.

Option 3 provides the ability to deploy Support Services to the SWIM Core, offering a major step forward toward net-centricity, including the ability to off-load ISS and other requirements to a common solution. This offers a significant step forward towards the vision of a net-centric NAS. This option lends itself to an incremental strategy that will allow the FAA to gain experience in applying net-centric technologies in the NAS.

In order to validate this recommendation and make a final decision for SWIM Segment 2 acquisition, the FAA should identify an initial set of Support and Interaction Services to be supported by the SWIM Core in Segment 2. Examples of candidates that have been discussed

recently include 4D weather cube data dissemination, on-demand NAS information services, surface data dissemination, and flight object dissemination. Once this initial set of services has been identified, a more detailed analysis can be performed to quantify the immediate cost and benefits of implementing a SWIM Core and deploying these services to this core, as opposed to the cost and benefits of implementing these services within NAS end systems, either as stand-alone functions or extending the SWIM Segment 1 federated approach. The analysis should also take into account the potential longer term benefits of initiating the development of the SWIM Core, including the security benefits obtained by conforming to an overarching NAS Security Architecture.

Once an initial set of Support and Interaction Services has been identified and validated for SWIM Segment 2, the necessary SWIM Core capabilities can be specified and acquired to support these services. These initial SWIM Core capabilities should be designed and implemented in a scalable manner, allowing addition of new capabilities as well as scaling up to support additional services and additional load.

Appendix A   Bibliography

1. Boan, Linda M, and others. *Initial Evolution Analysis for Achieving NAS Mid-Term Operations and Capabilities.* McLean, VA: The MITRE Corporation, September 2008.

2. Chappell, David. *Enterprise Service Bus.* O'Reilly Media Inc., June 2004.

3. Department of the Navy. "CANES SOA Reference Architecture, Version 2.0." August 2007.

4. FAA. *Exhibit 300: Attachment 3, Implementation Strategy and Planning, System Wide Information Management (SWIM) Program, Initial Submission.* Federal Aviation Administration, June 2007.

5. FAA. *NextGen 2025 System Interface Description SV-1P.* Washington, DC: Federal Aviation Administration_ATO-P Architecture Planning Group, March 2009.

6. FAA Order 1370.82A, Information Systems Security Program. September 2006.

7. *FAA SWIM Program - Segment 1 to Segment 2 Transition - Industry Input.* Arlington, VA: ITAA-GEIA, December 2008.

8. FAA. *System Wide Information Management (SWIM) Technical Overview, Version 1.1.* Washington, DC: Federal Aviation Administration, March 2008.

9. FAA, Information Security Certification and Accreditation (C&A) Package. March 2008.

10. Gregor Hophe, et. al. *Enterprise Integration Patterns, Designing, Building and Deploying Messaging Solutions.* Addison-Wesley, October 2003.

11. *Interface Requirements Document, SWIM/User, NAS-IR-43070001.* Washington, DC: Federal Aviation Administration, October 2008.

12. Joint Planning and Development Office-FAA. *Concept of Operatons for the Next Generation Air Transporation System, Version 2.0.* Washington, DC: Federal Aviation Administration, June 2007.

13. NIST. *Guide to Secure Web Services, SP 800-95, p 3-28.* National Institute of Standards and Technology, August 2007.

14. NIST. *Guidelines on Securing Public Web Servers, SP 800-44v2.* National Institute of Standards and Technology, September 2007.

15. Prabhu, Vikram, and Duncan Thomson. *Operational Concept for SWIM in the Mid-Term, MTR090073.* McLean, VA: MITRE, March 2009.

16. Reed, Harvey, and Keith McCaughin. *GCSS-AF Case Study.* McLean, VA: MITRE, March 2009.

17. Signore, Theodore, and others. *A NAS Security Architecture, MTR 090187.* McLean, VA: The MITRE Corporation, 2009.

18. *SWIM Core Services Enterprise Architecture Views, Draft Version 2.08.* Washington, DC: Federal Aviation Administration, April 2009.

19. *SWIM Final Program Requirements - Segment 1.* Washington, DC: Federal Aviation Administration, May 2007.

20. *SWIM Segment 2 Operation Services and Environment Definition, Version 1.0.* Washington, DC: Federal Aviation Administration, March 2009.

21. Wilkes, Lawrence. *Improving SOA Governance with the Systinet Business Services Registry.* CBDi Forum, April 2005.

Appendix B   NAS Information System Security Architecture

This section describes the emerging NAS Information System Security Architecture currently being created as part of the NAS Enterprise Architecture efforts, as it stands at the time of this writing. In this section we describe the major elements of the NAS Security Architecture and their relationship to the SWIM functional architecture.

Figure B-1 depicts a framework of major areas of ISS capability that need to be addressed by the NAS Security Architecture. These areas, together with supporting information technology (IT) capabilities and the capabilities of NAS end systems, contribute to the goal of providing the net-centric NAS mission services that support the operational concepts described in the NextGen concept of operations and implementation plan.
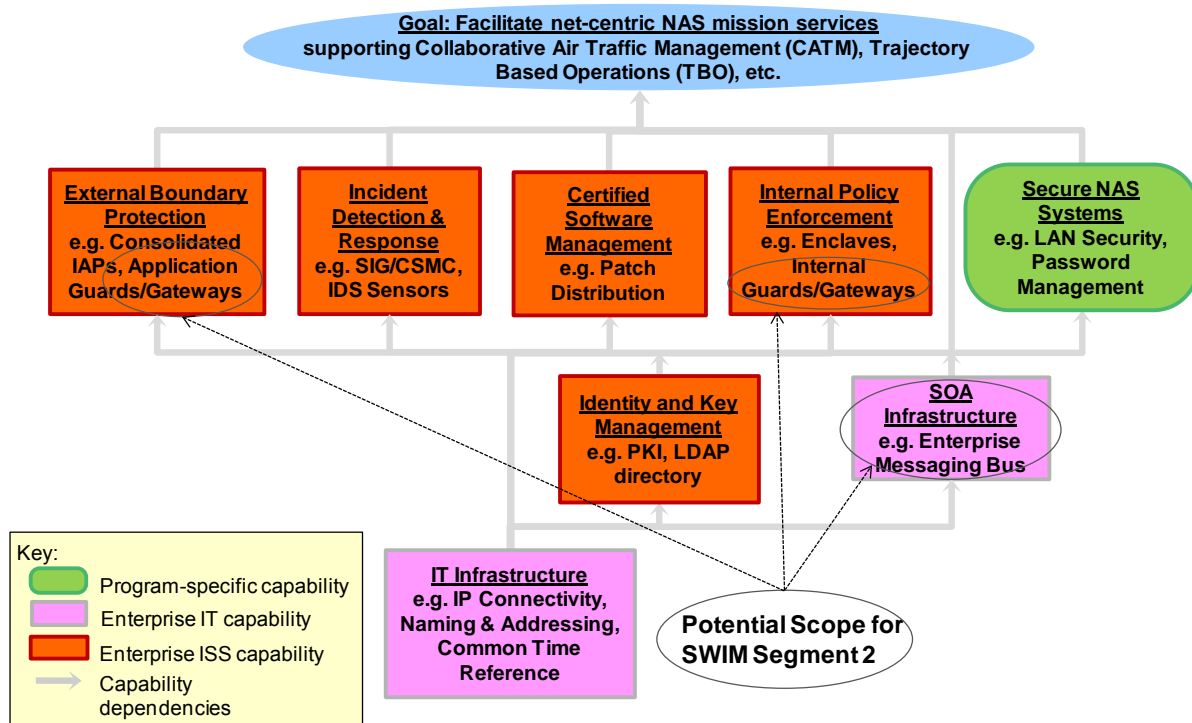
Figure B-1. NAS Security Architecture Framework

The major areas of the NAS IT and ISS capability shown in Figure B-1 are described below. For each area of capability, we provide a brief description of the area. We briefly describe how each capability relates to the SWIM functional architecture use in the main body of the document, which is based on the NAS Enterprise Services SV-4 functional decomposition.

Information Technology (IT) Infrastructure. This area consists of wide area and local area network infrastructure that provides network connectivity within the NAS, as well as other IT capabilities such as Data Storage.

The network services provided by the IT infrastructure are assumed to provide an assurance of integrity (no modification or insertion) of IP packets transmitted over the network, for all network communications. When specifically needed and ordered, the network services are also assumed to provide an assurance of confidentiality of IP packets transmitted over the network. IP network transport capabilities needed by SWIM include both Wide Area Network (WAN) and Local Area Network (LAN) capabilities. This includes support for the Internet Protocol Suite (IPS), including not just basic IP service but related services such as Domain Name System (DNS) services, and Network Time Protocol (NTP) services to provide common time reference. In addition, this area includes other IT capabilities such as computing platforms and data storage that are provided as enterprise services.

This capability area includes all of the items in the "Technical Infrastructure Services" layer of the NAS SV-4, with the exception of Boundary Protection, which is broken out separately below.

Identity and Key Management Infrastructure. This area includes capabilities for managing a Public Key Infrastructure (PKI) and managing information about identities of NAS operators (humans) and systems (devices). This is envisioned as a common infrastructure capability made available to support ISS functions in systems throughout the NAS.

This capability area is shown as "Identity and Key Management" in the NAS SV-4.

The functions in this capability area are described below, in increasing order of complexity:

- Providing and managing key materials[5] for devices, to support system-to-system authentication, confidentiality, and integrity functions throughout the NAS. This includes providing and managing server certificates (signed by a recognized authority) that may be used when a device needs to authenticate the identity of a peer device over the network. Key materials may also be used for confidentiality (encryption) and integrity (signing) of information to be passed from device to device over the network.

- Providing and managing key materials for individual users, to support user-to-system authentication, confidentiality, and integrity functions throughout the NAS. This includes providing and managing user certificates[6] that that are used when applications need to authenticate the identity of users connecting over the network. Key materials and certificates may also be used for confidentiality (encryption) and integrity (signing) of information to be passed over the network.

- Providing a central point for user authentication. This allows a user to authenticate their identity once, in such a way that multiple applications can rely on this identity in making access control decisions. (Provides support for "Single-sign on".)

---

[5] Managing key materials includes processes for issuance through revocation, and may include key validation services, for example services based on Online Certificate Status Protocol (OCSP).

[6] The solution for user identification and key management is assumed to be integrated with, and supported by, the FAA Personal Identification Verification (PIV) card. At the time of this writing, use of the PIV card for logical access control and identity management, as well as other functions, is being implemented for use in FAA administrative systems, by the LAACS program.

- Providing a capability for managing information about user identities, together with roles or user attribute information (policy management), and making this information accessible to systems throughout the NAS. This information, together with authenticated user identities supported by the key management capabilities described above, may be used in making access control decisions throughout the NAS.

- Access Control Management and Policy Decision Point (PDP) capability. This provides a centralized capability for managing rules about which users (by role or by attribute) are allowed to access which resources, and it allows systems throughout the NAS to refer access control decisions to a centralized PDP where these rules are applied.

SOA Infrastructure. This area consists of the SWIM core components (hardware and software), as well as SIP-provided components, that implement the SOA core services functions of the NAS SV-4.

Boundary Protection. This area includes controls to protect connections and information flows between NAS and non-NAS entities.

This area maps directly to the boundary protection function shown on the NAS SV-4 within "Technical Infrastructure Services". However, a complete boundary protection solution includes both network layer controls as well as application layer controls, and in this architecture we assume that SWIM core services will be used in building the application layer controls (for information flows that conform to SWIM standards, not necessarily for legacy flows), while other capabilities (in particular capabilities provided by FTI) will be used to provide network layer controls associated with boundary protection.

Internal Policy Enforcement. A key principle of the emerging NAS Security Architecture is that the NAS must be divided into enclaves, and that information flows crossing from one enclave to another must be subject to controls to ensure that only authorized (non-malicious) traffic is allowed to flow.

This capability is not currently shown on the NAS SV-4.

The need to perform internal policy enforcement creates a major driver on the SWIM architecture. In this architecture, we assume that the SWIM core is the point at which this internal policy enforcement takes place, at least for information flows that conform to SWIM standards (not necessarily for legacy flows). By making use of SOA core services, and the Identity and Key Management Infrastructure described above, the SWIM core can control the flow of information among NAS enclaves. (This assumes that the underlying IP network is configured to prevent direct system-to-system flows that would circumvent controls being applied in the SWIM core.) These controls would include:

- System/device-based access control. The SWIM core will allow NAS systems to access Mission and Support services based on the authenticated identity of the connecting system/device and policy (rules)

- User-based control of access to Interaction Services. The SWIM core will allows NAS systems to access Interaction services based on the authenticated user identity, roles or attributes associated with the user's identity, and policy (rules)

- Application Layer Guard Gateway processing. The SWIM Core will subject all messages/service requests passing through the SWIM core to schema-based validation[7] to ensure that the data content appears valid

Incident Detection and Response. This area includes instrumentation (e.g., network sensors and host based sensors) within the NAS to collect information that may indicate an intrusion or other security-related incident is happening, capabilities to monitor, analyze, and correlate this information, and capabilities to coordinate an effective response, including correcting the problem as well as performing activities such as reporting and forensics analysis.

There are several functions on the NAS SV-4 that relate to incident detection and response, in particular the Security Monitoring function within the SOA core services functional area.

Certified Software Management. This consists of a capability to provide approved software and patches, and to allow these to be distributed for use throughout the NAS in a secure manner.

This capability is not currently shown on the NAS SV-4.

The existence of a NAS Certified Software Management capability does not directly affect the SWIM Segment 2 Architecture – however it should be taken into account in the development of SWIM Segment 2 support concepts.

---

[7] SWIM schemas must be written in a restrictive manner, so that the expected valid content, and only valid content, can be identified.

Appendix C   Acronyms List

ACL   Access Control List

AG   Application Gateway

API   Application Program Interface

ATM   Air Traffic Management

ATO   Air Traffic Operations

BP   Boundary Protection

BPEL   Business Process Execution Language

C&A   Certification and Authorization

CATM   Collaborative Air Traffic Management

CBR   Content Based Routing

CertPath   Java Certification Path API

CM   Content Management

COI   Community of Interest

COTS   Commercial off-the-Shelf

CRL   Certificate Revocation List

CSMC   Cyber Security Management Center

DNS   Domain Name System (or Service)

DoD   Department of Defense

EA   Enterprise Architecture

EBP   External Boundary Protection

EMB   Enterprise Messaging Bus

ERAM   En Route Automation Modernization

ESB   Enterprise Service Bus

ESM   Enterprise Service Management

ETA   Estimated Time of Arrival

FAA   Federal Aviation Administration

FISMA   Federal Information Security Management Act

FPR   Final Program Requirements

FTI	FAA Telecommunications Infrastructure
GCSS-AF	Global Combat Support System – Air Force
GEIA	The industry consortium report
HA	Highly Available
HTML	Hyper Text Markup Language
HTTP	Hypertext and Transfer Protocol
HTTPS	HTTP over SSL
I&A	Identification and Authentication
ID	Identification
IM	Instant Messaging
IP	Internet Protocol
IPS	Internet Protocol Suite
IRD	Interface Requirements Document
ISS	Information System Security
IT	Information Technology
ITAA	Information Technology Association of America
J2SE	Java 2 Platform Standard Edition
JAAS	Java Authentication and Authorization Service
JAXB	Java Architecture for XML Binding
JAX-RS	Java API for RESTful Web Services
JAX-WS	Java API for Web Services
JBI	Java Business Integration
JCA	Java Cryptography Architecture
JCE	Java Cryptographic Extension
JGSS	Java Generic Secure Services
JMS	Java Messaging Service
JPDO	Joint Planning and Development Office
JRC	Joint Resources Council
JSSE	Java Secure Socket Extension
LAACS	Logical Access and Authorization Control Service

LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MITRE/CAASD	The MITRE Corporation, Center for Advanced Aviation System Development
MOM	Message-Oriented Middleware
MOU	Memorandum of Understanding
NAS	National Airspace System
NCES	Net Centric Enterprise Services
NextGen	Next Generation Air Transportation System
NGIP	Next Generation Implementation Plan
NIST	National Institute of Standards and Technology
NOC	Network Operations Center
NTP	Network Time Protocol
OCSP	On-Line Certificate Status Protocol
OI	Operational Improvement
OPS	Operations
OSED	Operation Services and Environment Definition
OSGi	Open Systems Gateway initiative
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PKI	Public Key Infrastructure
PLA	Program Level Agreement
QoS	Quality of Service
REG	Registry
REST	Representational State Transfer
RSS	Rich Site Summary
SAML	Security Authorization Markup Language
SASL	Simple Authentication and Security Layer
SDP	Service Delivery Point
SIG	Security Information Group
SIP	SWIM Implementing Program

SLA	Service Level Agreement
SOA	Service-Oriented Architecture
SOAP	Simple Object Access Protocol
SSL	Secure Sockets Layer
STA	Scheduled Time of Arrival
SV-4	NAS Enterprise Services functional hierarchy
SvSD	Service Specification Document
SWIM	System Wide Information Management
TCO	Total Cost of Ownership
TCP	Transmission Control Protocol
TFM	Traffic Flow Management
TLS	Transport Layer Security
UDDI	Universal Description, Discovery, and Integration
URL	Uniform Resource Locator
VoIP	Voice Over Internet Protocol
VPN	Virtual Private Network
WAN	Wide Area Network
WH	Web Hosting
WS-BPEL	Web Services Business Process Execution Language
WSDL	Web Services Description Language
WSF	Web Services Framework
WS-RM	WS-Reliable Messaging
Wx	Weather
XACML	eXtensible Access Control Markup Language
XKMS	XML Key Management Specification
XML	eXtensible Markup Language
XPATH	XML Path Language
XSLT	eXtensible Stylesheet Language Transformations